FRONTLINE TEST SYSTEM™

FTS4USB

USER MANUAL

Copyright © 2000-2010 Frontline Test Equipment, Inc. All rights reserved. You may not reproduce, transmit, or store on magnetic media any part of this publication in any way without prior written authorization of Frontline Test Equipment, Inc.

FTS, Frontline and Frontline Test System are registered trademarks of Frontline Test Equipment, Inc. Frontline is a trademark of Frontline Test Equipment, Inc.

All other trademarks and registered trademarks are property of their respective owners.

Table of Contents

1 Welcome to FTS ____ *1*

2 Getting Started ____ *3*

2.1 Control Window ____ **3**

2.2 The Control Window Toolbar ____ **3**

2.3 Drop-Down Menus ____ **4**

2.4 Configuration Information on the Control Window ____ **5**

2.5 Status Information on the Control Window ____ **5**

2.6 Frame Information on the Control Window ____ **6**

2.7 FTS4USB Data Capture Methods ____ **6**

2.8 Opening FTS4USB ____ **8**

3 Configuration Settings ____ *11*

3.1 Establishing the USB Hardware Settings ____ **11**

3.2 Internal Tap Datasource Dialog ____ **11**

3.3 Using the USB ComProbe® Datasource Dialog ____ **12**

3.3.1 Capture Filters ____ 12

3.3.2 Hardware Installation ____ 12

3.4 Troubleshooting USB Communications ____ **12**

3.5 USB ComProbe II ____ **13**

3.6 I/O Settings ____ **14**

3.6.1 USB I/O Settings ____ 14

3.6.2 USB I/O Settings - Digital Output Configuration ____ 15

3.7 Port Assignments ____ **17**

3.7.1 Adding or Changing Port Assignments ____ 17

3.8 Decoder Parameters ____ **17**

3.8.1 A2DP Decoder Parameters ____ 18

3.8.2 Security Parameters ____ 18

3.8.3 AVDTP Decoder Parameters ____ 20

3.8.4 L2CAP Decoder Parameters ____ 25

3.8.5 RFCOMM Decoder Parameters ____ 31

3.8.6 ROC Decoder Parameters ____ 37

3.8.7 USB Decoder Parameters ____ 42

3.8.8 Decoder Parameter Templates ____ 47

3.9 Spy Mode ____ **48**

3.9.1 Spy Mode Settings on the I/O Settings Dialog ____ 49

3.9.2 FIFOs and Spy ____ 49

3.9.3 Turning Off the FIFO Buffers ____ 50

3.10 CAN 2.0A Special Instructions ____ 51
3.10.1 CAN 2.0A Hardware Settings ____ 51
3.10.2 CAN 2/0A Capture Filters ____ 52
3.10.3 SST Woodhead DeviceNet Card Installation Instructions ____ 53

3.11 ControlNet Special Instructions for the 1784-PCC ____ 54
3.11.1 Capturing ControlNet Data ____ 54
3.11.2 ControlNet Setup ____ 55
3.11.3 ControlNet Statistics ____ 61

3.12 ControlNet Special Instructions for the 1784-U2CN ____ 61
3.12.1 ControlNet 1784-U2CN Hardware Settings ____ 61
3.12.2 ControlNet 1784-U2CN I/O Settings ____ 62

3.13 Data Highway Plus Special Instructions ____ 64
3.13.1 Data Highway Plus Setup for DL3500-DHM ____ 64
3.13.2 Special Instructions for 1784-U2DHP ____ 65

3.14 DeviceNet Special Instructions for the SST Woodhead interface cards ____ 67
3.14.1 DeviceNet I/O Settings ____ 67
3.14.2 DeviceNet Capture Filters ____ 68
3.14.3 SST Woodhead DeviceNet Card Installation Instructions ____ 70

3.15 DeviceNet Special Instructions for RA's 1784-U2DN interface device ____ 71
3.15.1 DeviceNet 1784-U2DN Hardware Settings ____ 71
3.15.2 DeviceNet 1784-U2DN I/O Settings ____ 72
3.15.3 DeviceNet 1784-U2DN I/O Settings - START/STOP Triggers ____ 73
3.15.4 Adding Simple Start/Stop Triggers ____ 73
3.15.5 ____ 74
3.15.6 Adding a Complex Start/Stop Trigger ____ 74
3.15.7 Editing a Simple Start/Stop Trigger ____ 76
3.15.8 Editing a Complex Start/Stop Trigger ____ 77
3.15.9 Deleting a Simple START/STOP Trigger ____ 77
3.15.10 Deleting a Complex Start/Stop Trigger ____ 77
3.15.11 IEC 870-5-101 & 104 Special Instructions ____ 78

3.16 Modbus Special Instructions ____ 80
3.16.1 Modbus Register Display Format Settings ____ 80
3.16.2 Setup For Modbus RTU and ASCII ____ 82
3.16.3 Setup for Modbus TCP ____ 83

3.17 Ethernet ComProbe Special Instructions ____ 83
3.17.1 Ethernet ComProbe Hardware Settings ____ 83
3.17.2 Ethernet ComProbe I/O Settings ____ 84

4 Protocol Stacks ____ 87

4.1 Protocol Stack Wizard ____ 87

4.2 Information Screen ____ 88

4.3 How the Analyzer Auto-traverses the Protocol Stack ____ 88

4.4 Creating and Removing a Custom Stack ____ 89

4.5 Saving User Defined Stacks ____ 90
4.6 Reframing ____ 91
4.7 Unframing ____ 91
4.8 Providing Context For Decoding When Frame Information Is Missing ____ 92
5 Capturing Data ____ 93
5.1 Capturing Data ____ 93
5.2 USB HCI Internal Software Tap Data Source Dialog ____ 94
6 Analyzing Byte Level Data ____ 95
6.1 Event Display ____ 95
6.2 The Event Display Toolbar ____ 95
6.3 Opening Multiple Event Display Windows ____ 97
6.4 Calculating CRCs or FCSs ____ 97
6.5 Calculating Delta Times and Data Rates ____ 99
6.6 Switching Between Live Update and Review Mode ____ 99
6.7 Data Formats and Symbols ____ 99
6.7.1 Switching Between Viewing All Events and Viewing Data Events ____ 99
6.7.2 Switching Between Hex, Decimal, Octal or Binary ____ 100
6.7.3 Switching Between ASCII, EBCDIC, and Baudot ____ 100
6.7.4 Viewing Only ASCII (or EBCDIC or Baudot) ____ 100
6.7.5 Viewing Only Hex (Or Decimal or Octal or Binary) ____ 101
6.7.6 Selecting Mixed Channel/Sides ____ 101
6.7.7 List of All Event Symbols ____ 101
6.7.8 Font Size ____ 103
7 Analyzing Protocol Decodes ____ 105
7.1 Frame Display Window ____ 105
7.1.1 Frame Display Window ____ 105
7.1.2 Frame Display Toolbar ____ 106
7.1.3 Frame Display Status Bar ____ 109
7.1.4 Hiding and Revealing Protocol Layers in the Frame Display ____ 109
7.1.5 Physical vs. Logical Byte Display ____ 109
7.1.6 Sorting Frames ____ 110
7.1.7 Synchronizing the Event and Frame Displays ____ 110
7.1.8 Working With Multiple Frame Displays ____ 110
7.1.9 Working With Panes ____ 111
7.1.10 The Panes in the Frame Display ____ 111
7.1.11 Protocol Layer Colors ____ 116
7.1.12 Protocol Filtering from the Frame Display ____ 117
7.2 Protocol Navigator Window ____ 119
7.2.1 Protocol Navigator ____ 119

7.2.2 Protocol Navigator Toolbar 120
7.2.3 Protocol Navigator Status Bar 122
7.2.4 The Difference Between Filtering and Hiding 122
7.2.5 Hiding and Revealing Protocol Layers in the Protocol Navigator 122
7.2.6 Filtering on a Protocol Layer 123
7.2.7 Filtering on all Frames with Errors from the Protocol Navigator 123
7.2.8 Expanding and Collapsing Protocol Layers 124

8 Analyzing Control Signal Changes 127

8.1 Viewing Signal Changes in Real-time 127
8.1.1 Breakout Box Window 127
8.1.2 The Breakout Box Toolbar 128
8.1.3 Reading the Breakout Box Window 129
8.1.4 Selecting Breakout Box Options 129

9 Viewing Historical Signal Changes 131

9.1 Signal Display Window 131

9.2 Signal Display Toolbar 132

9.3 Reading the Signal Display 132

9.4 Selecting Signal Display Options 134

10 Statistics 135

10.1 Statistics 135

10.2 Statistics Window 135

10.3 Session, Resettable and Capture File Tabs 135

10.4 Copying Statistics To The Clipboard 136

10.5 Graphs 136
10.5.1 Statistics Graphs 136
10.5.2 Printing Graphs 137
10.5.3 Changing the Graph Refresh Rate 137
10.5.4 Viewing Percentages or Values 137

10.6 Information on Tables 137
10.6.1 Statistics Tables 137
10.6.2 Bytes Per Second Table 138
10.6.3 Frames Per Second Table 138
10.6.4 Characters Per Second Table 139
10.6.5 Utilization Table 139
10.6.6 Data Table 140
10.6.7 Unfiltered Data Table 141
10.6.8 Octets Per Second Table 141
10.6.9 Buffer Information Table 142
Errors Table 142

10.7 Packet Error Rate Statistics (PER Stats) 145
10.7.1 Packet Error Rate 145

10.8 Data Highway Plus Statistics ____ 147
10.8.1 Starting DH+ Statistics ____ 147
10.8.2 Overview Dialog ____ 147
10.8.3 Individual Device Statistics ____ 153
10.8.4 Network Statistics ____ 156
10.8.5 DH+ Statistics Files ____ 167

11 Transmitting Data ____ 169

11.1 Transmit Window ____ 169
11.2 Transmitting Strings ____ 169
11.3 Transmitting Files ____ 170
11.4 Transmitting FTS Capture Files ____ 170
11.5 The Transmit Toolbar ____ 171
11.6 String Formats ____ 172
11.7 Flow Control when Transmitting ____ 173
11.8 Changing Control Signals ____ 174
11.9 Delays and Max Burst Size ____ 174
11.10 Transmit Options ____ 176
11.11 Pause Transmit ____ 176

12 Coexistence View ____ 177

12.1 Coexistence View Introduction ____ 177
12.1.1 Average Throughput/1 Second Throughput ____ 177
12.1.2 Throughput Graph ____ 178
12.1.3 Legend ____ 179
12.1.4 Coexistence View Wi-Fi Tx Address ____ 179
12.1.5 Timeline ____ 181
12.2 Coexistence button bar ____ 182
12.3 Bluetooth® Channel Frequencies ____ 183
12.4 Wi-Fi Channel Frequencies - 2.4 GHz Channels ____ 184
12.5 Wi-Fi Channel Frequencies - 5 GHz Channels ____ 185

13 Bluetooth Timeline ____ 187

13.1 Bluetooth® Timeline ____ 187
13.2 Bluetooth® Timeline Packet_Depiction ____ 188
13.3 Bluetooth® Timeline Packet Navigation and Selection ____ 191
13.4 Bluetooth® Timeline Button Bar ____ 191
13.5 Bluetooth® Timeline Menu Bar ____ 192

13.6 Bluetooth® Timeline Visual Elements 194
13.7 Bluetooth® Timeline Zooming 196
13.8 Bluetooth® Timeline Throughput Displays 197
13.9 Bluetooth® Timeline Average Throughput Indicators 197
13.10 Bluetooth® Timeline One Second Throughput Indicators 197
13.11 Bluetooth® Timeline Throughput Graph 198
13.12 Bluetooth® Timeline Discontinuities 199
13.13 Legend 199
14 low energy Timeline 200
14.1 low energy Timeline Introduction 200
14.2 Bluetooth® low energy Timeline Packet Depiction 200
14.3 Navigating and Selecting Data 201
14.4 Button Bar 202
14.5 Menu Bar 203
14.6 Visual Elements 205
14.7 Zooming 206
14.8 Throughput Displays 207
14.9 Packet Throughput 207
14.10 Payload Throughput 208
14.11 Packet/Payload Throughput 208
14.12 Throughput Graph 209
14.13 Discontinuities 210
14.14 Legend 210
15 Network View 211
15.1 Network View Introduction 211
15.2 Display Node Information in Network View 211
15.3 Displaying Conversation Information in Network View 213
15.4 Adding/Editing an Alias for a Node in Network View 214
15.5 Filter and Sort the Network View 214
15.6 Setting The Count For Top N Filters 215
15.7 Detail Window Layouts in Network View 216
15.8 The Statistics Graph Window in Network View 219

15.9 The Network View Node Database 219

15.10 Resolving DNS Names in Network View 220

15.11 The Network View Toolbar 220

15.12 Network View Visual Elements 221

15.13 Network View Technical Notes 222

15.14 Network View - Frame Sizes 226

16 NetDecoder Dashboard 227

16.1 Dashboard 227

16.1.1 One Hour/Ten Minute Chart 228
16.1.2 Dashboard: Utilization (Percentage of Bandwidth) and Throughput (Percentage of Actual Traffic) 228
16.1.3 Top Talkers Bar Chart 229
16.1.4 Show DNS Names 229
16.1.5 Bandwidth Drop-down 230
16.1.6 Network Utilization Meter 230
16.1.7 Bad Packets Meter 230
16.1.8 % Top Utilization/Top Utilizer Meter 230
16.1.9 Charts 231
16.1.10 Network Alarms (Utilization) 231
16.1.11 App Distribution (Utilization/Throughput) 232
16.1.12 IP Addresses 232
16.1.13 Dashboard - Define Applications and Alarms 233
16.1.14 Define Email Addresses 234
16.1.15 Dashboard - Define Authorized IP Addresses 234
16.1.16 Dashboard - Show IP Addresses Seen 235

17 Audio Extraction 237

17.1 Audio Extraction 237

17.2 Audio Extraction Settings 237

17.3 Enable Live WAV File Creation 237

17.4 Export WAV File 238

17.5 File Naming 238

17.6 Status Dialog 238

18 Data Extraction 239

18.1 Data Extraction 239

18.2 Data Extraction Settings 239

19 Find 241

19.1 Starting a Search 241

19.2 Using Go To 241

19.3 Searching for Control Signal Changes 243
19.4 Searching for Data Errors 245
19.5 Searching for Frame Errors 247
19.6 Searching for Special Events 248
19.7 Searching within Decodes 249
19.8 Side Restrictions 250
19.9 Searching by Signal 252
19.10 Changing Where the Search Lands 252
19.11 Subtleties of Timestamp Searching 253
19.12 Entering Search Patterns (String Searches) 253
19.12.1 Searching by Pattern 253
19.12.2 Entering Characters 254
19.12.3 Entering Hex or Binary 255
19.12.4 Control Characters 255
19.12.5 Wildcard Character 255
19.12.6 Examples of Search Strings 255
19.13 Searching by Time 256
19.13.1 Searching by Time 256
19.13.2 Searching with Absolute Timestamp 257
19.13.3 Searching with Relative Timestamp 258
19.13.4 Choosing "On or Before" or "On or After" 259
20 Bookmarks 261
20.1 Bookmarks 261
20.2 Adding, Modifying or Deleting a Bookmark 261
20.3 Displaying All and Moving Between Bookmarks 262
21 Filtering 263
21.1 Difference Between Ethernet Capture Filters and Display Filters 263
21.2 Display Filters 263
21.2.1 About Display Filters 263
21.2.2 Including and Excluding Radio Buttons 264
21.2.3 Creating a Display Filter 264
21.2.4 Named Display Filters 265
21.2.5 Using Compound Display Filters 265
21.2.6 Defining Node and Conversation Filters 266
21.2.7 Using Advanced Display Filtering Techniques 267
21.2.8 Deleting and Hiding Display Filters 267
21.2.9 Editing Filters 269
21.3 Ethernet Capture Filters 270
21.3.1 Creating and Using an Ethernet Capture Filter 270

21.3.2 Applying an Ethernet Capture Filter 271
21.3.3 Removing an Ethernet Capture Filter 271
21.3.4 Defining Node and Conversation Ethernet Capture Filters 272
21.3.5 Selecting Predefined Ethernet Capture Filters 272
21.3.6 Defining Pattern or Offset Ethernet Capture Filters 273
21.3.7 Using BPF to Create a Custom Ethernet Capture Filter 273
21.3.8 Creating/Deleting a Compound Filter 274
21.3.9 Naming Ethernet Capture Filters 274
21.3.10 Modifying a Condition in an Ethernet Capture Filter 275
21.3.11 Deleting a Condition in an Ethernet Capture Filter 275
21.3.12 Filter Formats 275
21.3.13 Saving and Loading Capture Filter Files 281

21.4 Protocol Filtering from the Frame Display 282
21.4.1 Easy Protocol Filtering 282
21.4.2 Filtering On the Summary Layer Protocol 282
21.4.3 Quick Filtering on a Protocol Layer 283
21.4.4 Filtering on all Frames with Errors from the Frame Display 284

21.5 Protocol Filtering from the Protocol Navigator 284
21.5.1 Filtering on a Protocol Layer 284
21.5.2 Filtering on all Frames with Bookmarks 284
21.5.3 Filtering on all Frames with Errors from the Protocol Navigator 285
21.5.4 Filtering on all Frames with Special Information Nodes 285
21.5.5 Named Filters 285

22 Saving Data 287

22.1 Saving Your Data 287

22.2 Saving the Entire Capture File using File > Save or the Save icon 287

22.3 Saving the Entire Capture File with Save Selection 288

22.4 Saving a Portion of a Capture File 289

22.5 Confirm Capture File (CFA) Changes 290

22.6 Adding Comments to a Capture File 291

23 Loading and Importing Capture Files 293

23.1 Loading a Capture File 293

23.2 Importing Capture Files 293

23.3 Converting Timestamps 294

23.4 Adding Comments to a Capture File 294

23.5 File Format for Merlin Files 295

24 Printing 297

24.1 Printing from the Frame Display/HTML Export 297

24.2 Frame Display HTML Export 299

24.3 Printing from the Event Display ____ 300

24.4 Print Preview ____ 302

25 Exporting ____ 305

25.1 Export ____ 305

25.2 Export Filter Out ____ 305

25.3 Exporting Event Display to a File ____ 305

25.4 Exporting Baudot ____ 307

25.5 HTML Export ____ 307

26 System Settings and Program Options ____ 309

26.1 System Settings ____ 309

26.2 System Settings - Disabled/Enabled Options ____ 311

26.3 Bluetooth ComProbe Maintenance ____ 311

26.4 Advanced System Options ____ 312

26.5 Changing Default File Locations ____ 313

26.6 Selecting Start Up Options ____ 314

26.7 Names ____ 315

26.8 Timestamping ____ 316

26.8.1 Timestamping Options ____ 316
26.8.2 Enabling/Disabling Timestamping ____ 316
26.8.3 Switching Between Relative and Absolute Time ____ 317
26.8.4 Changing the Timestamping Resolution ____ 317
26.8.5 Displaying Fractions of a Second ____ 318
26.8.6 Converting Timestamps ____ 318
26.8.7 Performance Issues For High Resolution Timestamps ____ 318

27 Technical Information ____ 321

27.1 Contacting Technical Support ____ 321

27.2 Performance Notes ____ 321

27.3 Asynchronous Serial Performance Notes ____ 322

27.4 Synchronous Serial Performance Notes ____ 324

27.5 Ethernet Performance Notes ____ 325

27.6 BT Snoop File Format ____ 326

27.7 Changing Where the Search Lands ____ 329

27.8 Progress Bars ____ 330

27.9 Event Numbering ____ 330

27.10 File Format for Merlin Files ____ 330

27.11 Flag and Sync Character Subtleties ____ 331

27.12 Known Issues with the Source BD_ADDR Field ____ 331

27.13 Ring Indicator ____ 331

27.14 Padding of Short Frames ____ 332

27.15 RS-232 Pin-outs ____ 332

27.16 CRC! ____ 333

27.17 BPF Copyright Notice ____ 333

27.18 Useful Character Tables ____ 334

27.18.1 ASCII Codes ____ 334
27.18.2 Baudot Codes ____ 335
27.18.3 EBCDIC Codes ____ 335
27.18.4 Communication Control Characters ____ 336

27.19 The Serial Driver ____ 337

27.19.1 The FTS Serial Driver ____ 337

27.20 Frame Decoder ____ 338

28 Index ____ 339

1 Welcome to FTS

Welcome to Frontline Test System (FTS). The design of FTS allows you to conduct data analysis of protocols using your personal computer. The FTS interface is easy to use without training, but we recommend you read the online Help to take maximum advantage of all the features.

We designed the online Help System with complete explanations and easy to use systematic instructions. Access the online Help by choosing Help Topics from the Help menu, or by pressing the F1 key on any window.

2 Getting Started

2.1 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The *Control* window provides access to each window as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function.

Because the *Control* window can get lost behind other windows, every window has a *Home* icon  that brings the *Control* window back to the front. Just click on the *Home* icon to restore the *Control* window.

When running the *Capture File Viewer*, the *Control* window toolbar and menus contain only those selections needed to open a capture file and display the About box. Once a capture file is opened, the analyzer limits Control window functions to those that are useful for analyzing data contained in the current file. Because you cannot capture data while using *Capture File Viewer*, data capture functions are unavailable. For example, when viewing Ethernet data, the Signal Display is not available. The title bar of the Control window displays the name of the currently open file. The status line (below the toolbar) shows the configuration settings that were in use when the capture file was created.

2.2 The Control Window Toolbar

Available options are in color, while unavailable options are grayed out. All toolbar icons have corresponding menu items. Toolbar icon displays vary according to operating mode and/or data displayed.

 Open File - Opens a capture file.

 I/O Settings - Opens the I/O Settings dialog.

 Start Capture - Begins data capture to disk.

 Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.

 Clear - Clears or saves the capture file.

 Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.


Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.


Protocol Navigator - (framed data only) Opens the Protocol Navigator window, with the currently selected frame highlighted.


Statistics Window - Opens up the Statistics window.


Signal Display - Opens The Signal Display dialog.


Breakout Box - Opens the Breakout Box dialog.


Transmit - Opens the Transmit dialog.


Cascade - Arranges windows in a cascaded display.


Packet Timeline - Opens the Packet Timeline display.


Extract Data - Opens the Extract Data dialog.


Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.

2.3 Drop-Down Menus

The menus that you see on the Control Window and dialogs like Frame Display and Event Display vary depending on whether the data is being captured live or whether you are looking at a .cfa file. You will see File, View, Live, Options, Window, and Help. Most of the options are self explanatory.

- Many of the **File** menu items are standard Windows type commands: Open, Close, Save, Recent Files, etc. There are two exceptions:
    - **Recreate Companion File**. This option is available when you are working with decoders. If you change a decoder while working with data, you can use Recreate Companion File to recreate the .frm file, the companion file to the .cfa file. Recreating the .frm file helps ensure that the decoders will work properly.

- **Reload Decoders**. When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded.

- Under the **View** menu you can choose which FTS windows are available to open.

- **Live** contains commands that used in capturing data.

- Under **Options** you have opportunities to set/modify various system settings.

- The **Window** menu displays the open FTS dialogs and standard options like Cascade, Minimize, Tile, etc.

- Within the **Help** menu you can open the electronic Help file, About FTS, and access the FTS web site for additional help.

2.4 Configuration Information on the Control Window

The *Configuration* bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc. If the analyzer cannot find the MAC Address, it lists zeroes after the NIC name.



2.5 Status Information on the Control Window

The *Status* bar located just below the *Configuration* bar on the *Control* window provides a quick look at current activity in the analyzer.



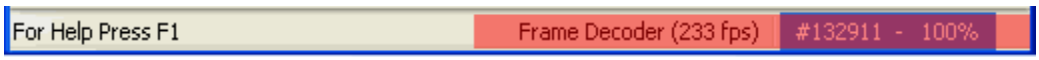
- *Capture Status* displays *Not Active*, *Paused* or *Running* and refers to the state of data capture.
  - *Not Active* means that the analyzer is not currently capturing data
  - *Paused* means that data capture has been suspended
  - *Running* means that the analyzer is actively capturing data.

- % Used
    - The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200K capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to overwrite the oldest data, depending on the choices you made in the System Settings.

- Utilization/Events
    - The second half of the status bar gives the current utilization and total number of events seen on the network. This is the total number of events monitored, not the total number of events captured. The analyzer is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.

2.6 Frame Information on the Control Window

Frame Decoder information is located just below the *Status* bar on the *Control* window. It displays two pieces of information.



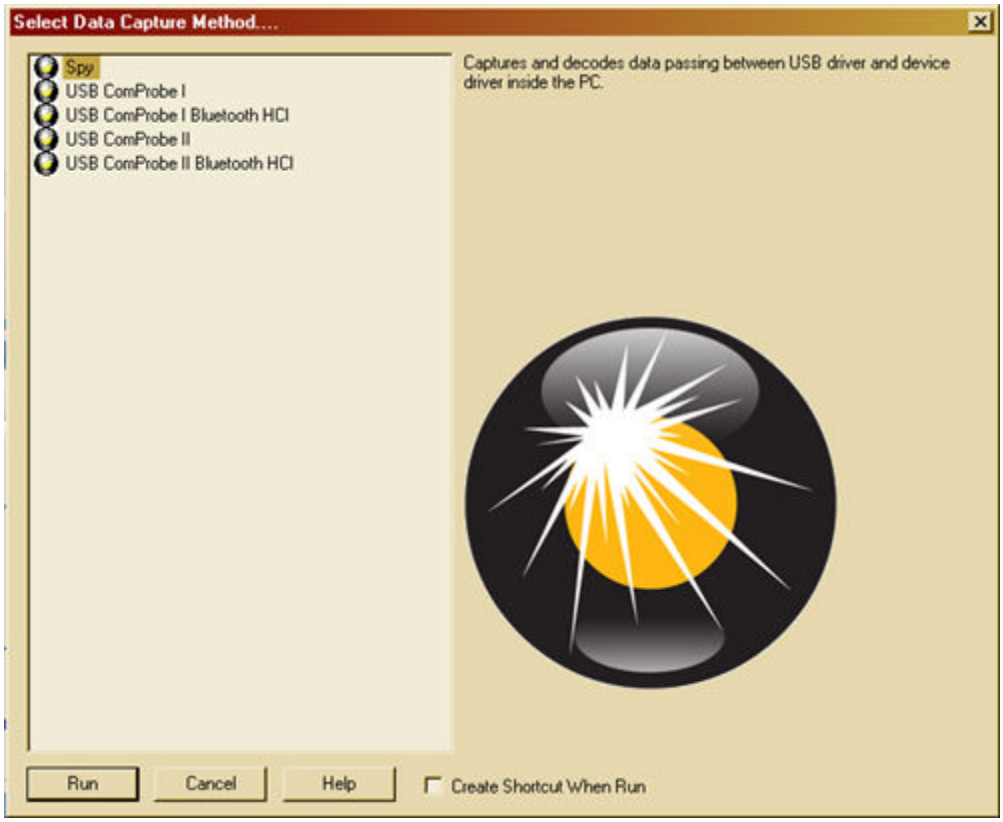
- **Frame Decoder (233 fps)** displays the number of frames per second being decoded. You can toggle this display on/off with Ctrl-D, but it is available only during a live capture.

- **#132911** displays the total frames decoded.

- **100%** displays the percentage of buffer space used.

2.7 FTS4USB Data Capture Methods

FTS4USB has different data capture methods to accommodate various applications. In the list below, folder names are in bold type, and data capture shortcuts are in normal type. Selecting any of the shortcuts activates the "Run" button at the bottom of the dialog.



The Protocols available for selection include:

- **Spy**
  Captures and decodes data passing between USB driver and device driver inside the PC.

- **USB ComProbe I**
  Captures and decodes USB bus activities and transactions.

- **USB ComProbe I Bluetooth HCI**
  Captures and decodes Bluetooth data - USB and USB Setup data will be filtered out.

- **USB ComProbe II**
  Captures and decodes USB bus activities and transactions.

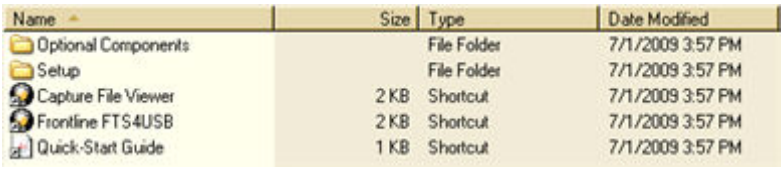
- **USB ComProbe II Bluetooth HCI**
  Captures and decodes Bluetooth data - USB and USB Setup data will be filtered out.

2.8 Opening FTS4USB

On product installation, the installer creates a folder on the windows desktop labeled **Frontline FTS4USB**.

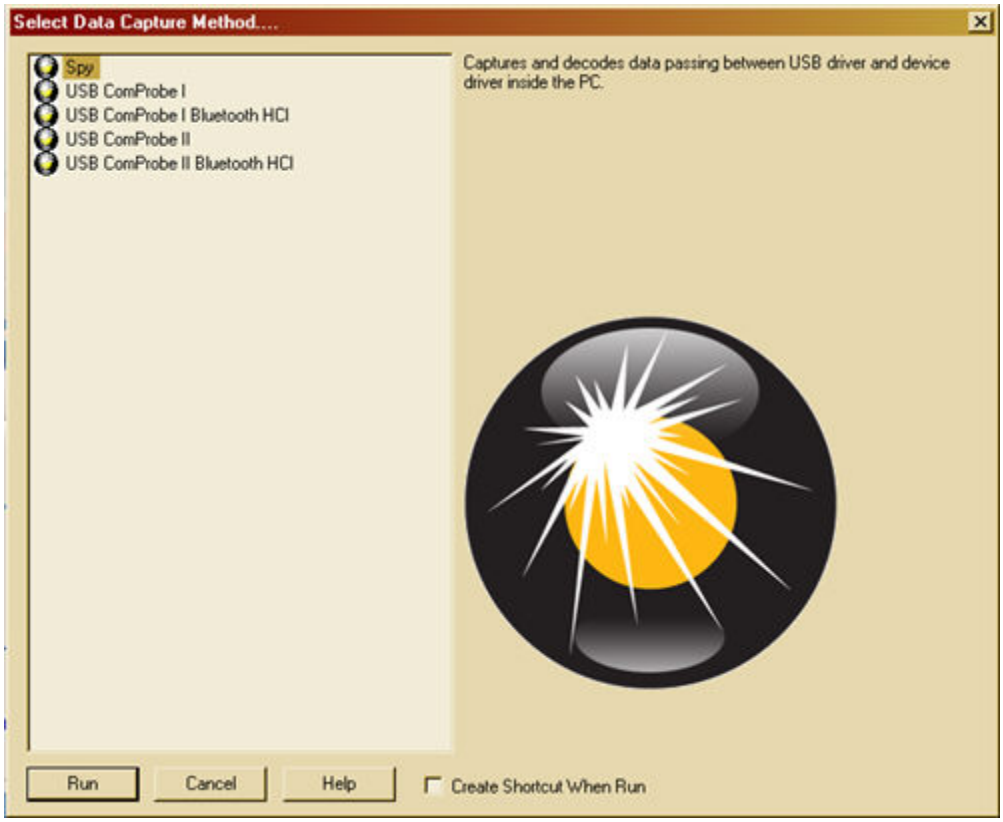
1. Double-click the Frontline FTS4USB *desktop folder*. 

This opens a standard Windows file folder window.



Name	Size	Type	Date Modified
Optional Components		File Folder	7/1/2009 3:57 PM
Setup		File Folder	7/1/2009 3:57 PM
Capture File Viewer	2 KB	Shortcut	7/1/2009 3:57 PM
Frontline FTS4USB	2 KB	Shortcut	7/1/2009 3:57 PM
Quick-Start Guide	1 KB	Shortcut	7/1/2009 3:57 PM

2. Double-click on Frontline FTS4USB and the system displays the *Select Data Capture Method* dialog..



This dialog lists all the methods FTS4USB supports in a tree control.

Three buttons appear at the bottom of the dialog; **Run**, **Cancel**, and **Help**. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).

Run starts FTS using the selected protocol stack.

Cancel closes the dialog and exits the user back to the desktop.

Help takes the user to this help file as does pressing the F1 key.

3. Expand the folder and select the data capture method that matches your configuration.

Note: If you don't need to identify a capture method, then click the Run button to start the analyzer.

Creating a Shortcut

A checkbox labeled **Create Shortcut When Run** is located near the bottom of the dialog. This box is un-checked by default. Select this checkbox, and the system creates a shortcut

for the selected method, and places it in the FTS4BT desktop folder and in the start menu when you click the Run button. This function allows you the option to create a shortcut icon that can be placed on the desktop. In the future, simply double-click the shortcut to start the analyzer in the associated protocol.

Note: You can also open the application by selecting *Start > All Programs > Frontline FTS4USB (Version #) > FTS4USB Spy*, *USB ComProbe I,* or *USB ComProbe II* .Minimizing Windows

Windows can be minimized individually or as a group when the *Control* window is minimized.

To minimize windows as a group:

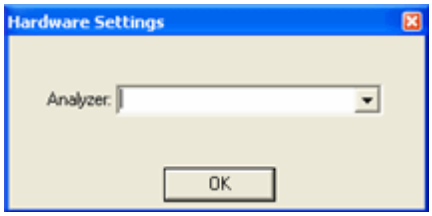
1. Go to the *Window* menu on the *Control*  window
2. Select *Minimize Control Minimizes All*. The analyzer puts a check next to the menu item, indicating that when the Control window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

3 Configuration Settings

3.1 Establishing the USB Hardware Settings

When establishing USB settings, you must select which device to sniff.

1. Connect the USB ComProbe® to an available USB port.
2. Start the analyzer.
3. Click the Hardware Settings button and select which USB ComProbe to use.



Choose a USB ComProbe device to use from the drop down list. If you just have one USB ComProbe connected to your PC, that device is used automatically and you don't need to select it.

4. Start data capture. On the Control Window, click *Start Capture* icon  .

Check the I/O Settings dialog to select the packet types filtered out of the capture.

3.2 Internal Tap Datasource Dialog

The USB Data Source Dialog allows the user to initiate or terminate the sniffing process on a USB device.

This dialog has a list control containing the USB Devices connected to your system. If the *Show Connected Only* checkbox is unchecked then all USB devices that have ever been connected to your system are listed.

The *Refresh List* button updates the list if you have connected or disconnected a device while this dialog is open.

To initiate the sniffing process:

1. Select the device you wish to sniff then click on the *Start Sniffing* button.
2. Click on the *Start Capture to Disk* icon on the Control window to capture data.

3.3 Using the USB ComProbe® Datasource Dialog

The USB Datasource Dialog allows the user to initiate or terminate the sniffing process on a select USB packet sniffer device . The dialog has a list control showing the USB Devices connected to your system. If you have connected or disconnected a device, click Refresh List to update the list

To start the sniffing process:

1. Choose a USB ComProbe device to use from the drop down list. If you only have one ComProbe connected to your PC, that device is used automatically and you don't need to select it.
2. Click the *Start* button to start the sniffing process,
3. Click on the *Start Capture to Disk* button on the Control window to capture data.

3.3.1 Capture Filters

FTS filters out a number of packet types by default. If you would like to view these packet types :

1. Click the *Capture Filters* button
2. Un-check the box next to the type of packet you wish to include in your results.

Some of these packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display and Protocol Navigator windows.

3.3.2 Hardware Installation

Consult the Quick Start Guide for information on installing the USB ComProbe.

To access the PDF version of the Quick Start Guide from your Windows operating system:

1. Click Start | Programs | FTS4USB [version #] | Quick Start Guide, or locate it in the FTS4USB desktop folder.

3.4 Troubleshooting USB Communications

Most performance problems such as input buffer overflow are the result of improper connections.

To achieve optimal performance from the USB analyzer, we recommend the following configuration:

- Use two high-speed computers, one for the analyzer and one for the device under test.
- Use USB 2.0 connections.
- Use cables that do not exceed the recommended maximum lengths (the cable connected to the analysis computer should not exceed 15 feet, and the total length of the cables connected to the test computer and the device under test should not exceed 9 feet).

Although it is possible to use one computer as both the analysis and the test computer, this requires that the computer in use is high-speed and has two or more host controllers available. If you attempt to analyze data using one computer with only one host controller, then the system displays an error message informing you of the problem.

If the operating system encountered an error when trying to install a device, simply disconnect the device, then reconnect it and try again.

Negative Timestamp Delta Value

On rare occasions, the system may display a negative delta value. One possible explanation has to do with the Reset function. The timestamp occurs when the Reset is actually sent but perhaps as much as 10 ms might pass before the Reset takes effect. Only then does the Datasource send the Reset up to the analyzer, and thus the negative delta.

USB HCI – Internal Tap FTS4USB Spy Mode

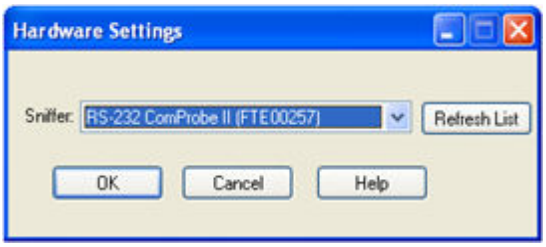
Sniffing USB devices without the aid of a USB ComProbe® can be troublesome. Some of the data, such as file transfers when sniffing flash drives, are often missed when sniffing USB devices directly causing the analyzer to ignore subsequent data. If the analyzer appears to stop processing data from a USB device when running in "Internal TapSpy" mode, then simply install a USB ComProbe, restart the packet sniffer, and the system should function normally.

3.5 USB ComProbe II

The Hardware Settings dialog is used to select a device to sniff/scan.

To access the Hardware Settings dialog:

1. Select *Hardware Settings* from the Options menu on the Control window.



2. Select *a device* from the drop-down list.
3. Select *OK.*

If no devices are found, the list will be blank. You can also select Refresh List to make sure the list is complete.

3.6 I/O Settings

3.6.1 USB I/O Settings

The IO Settings dialog is used to configure a configure device in FTS4USB. The USB ComProbe® filters out a number of packet types by default.

Hardware Input Filter

These options will enable the analyzer hardware to discard some common packet groups to reduce the amount of capture data received. Some of these packet groups correspond to polling operations and so these sequences do not contain any actual data transfer. If there is a change in the digital input lines in the middle of one of the packet groups that is being filtered, that group will not be discarded. In this way, the context for the digital input line change is preserved.

1. Select a checkbox to filter out one or more of the following packets..

- SOF – Discard Start-of-Frame packets. This setting is on by default.
- Poling IN packets
- IN+ACK IN+NAK
- PING+NAK
- PRE – Discard all PRE tokens.
- SPLIT – Enabling this option will cause the hardware to discard many polling split packet groups. The split groups that will be discarded are:
  - – SSPLIT+IN
  - – SSPLIT+IN+ACK
  - – CSPLIT+IN+NAK
  - – CSPLIT+IN+NYET
  - – CSPLIT+OUT+NYET
  - – CSPLIT+SETUP+NYET
- All bus activity
- Chrip J/K pairs

- Keep alives
- Packets

Digital Input Enabling Options

Digital inputs provide a means for users to insert events into the data stream. There are four digital inputs that can be enabled individually. Whenever an enabled input changes state it will issue an event and be tagged with a timestamp of when the input was interpreted by the analyzer. Digital inputs can not exceed a rate of 30 MHz. Digital inputs that occur faster than that are not guaranteed to be interpreted correctly by the analyzer. Also, only one digital input event may occur per active packet. All other digital input events can only be handled after the packet has completed. Digital inputs, although guaranteed to have the correct timestamp given the previous conditions, have the possibility of being presented out of order because they are provided randomly by the user and have no direct correlation to the bus. It is important to note that the digital inputs are susceptible to cross-talk if they are not being actively driven. A situation like this could occur if a digital input has been enabled, but has not been tied to a signal. Any other nearby signal (i.e., other digital inputs or outputs) could cause the input to activate. It is recommended that all undriven digital inputs be disabled or tied to ground.

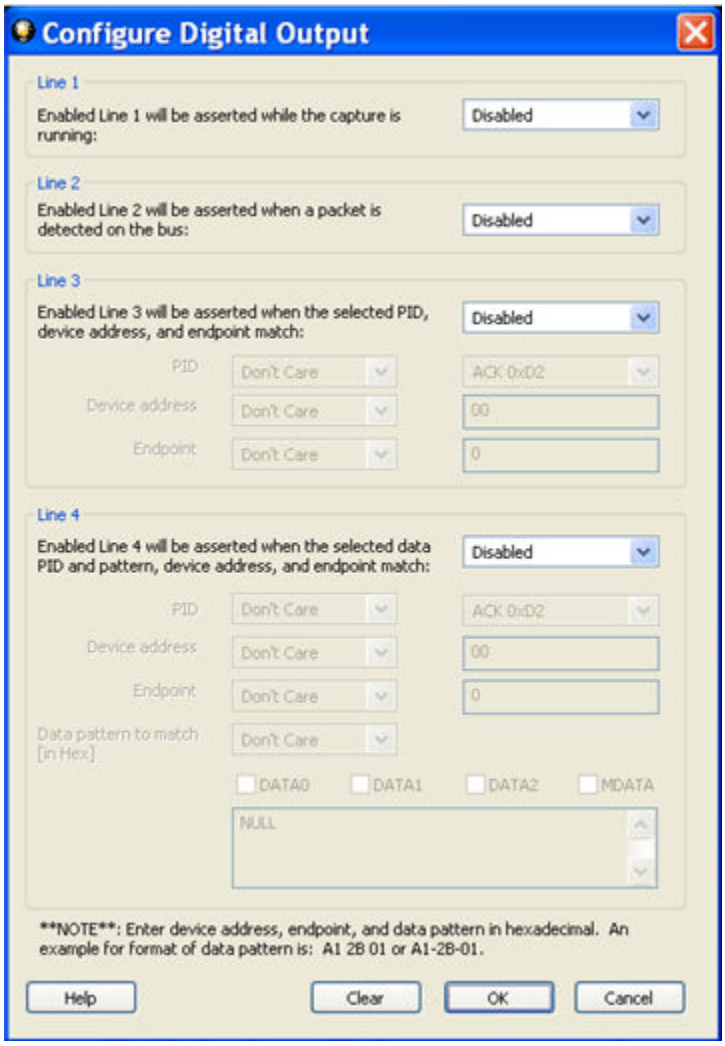
2. Select one or more of the Input options

Digital Output Configuration

3. Select the Configure button to set the output configuration.

3.6.2 USB I/O Settings - Digital Output Configuration

Digital outputs provide a means for users to output certain events to other devices, such as oscilloscopes. In this way, users can synchronize events on the bus with other signals they may be measuring.



There are four digital outputs that are user configurable. Each output has the option of being Enabled/Disabled, Active High (voltage), or Active Low (voltage).



Furthermore, each output can activate on specific conditions. Click on the links below to learn about each Output is activated.

- Digital Output 1
- Digital Output 2
- Digital Output 3
- Digital Output 4

3.7 Port Assignments

3.7.1 Adding or Changing Port Assignments

The analyzer autotraverses the stack from TCP, UDP and IPX based on the source or destination port number. Many systems use user-defined port numbers for both standard and custom protocols. Here's how to tell the analyzer about a custom port assignment on the system you are monitoring.

Add a New Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control  window.
2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Choose the *Single Port* radio button, and enter the port number in the *Port Number* box.
4. In the *Protocol* drop-down list, choose the protocol to traverse to.
5. Click the *Add* button. The system adds new entry to the bottom of the port number list.

Modify an Existing Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window.
2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Select (click on and highlight) the port assignment to modify.
4. Change the port number and/or choose the protocol to traverse to.
5. Click the *Modify* button. The system displays the changes in port number list.
6. You can also specify a range of ports. Select the *Port Range* radio button and specify the starting and ending port numbers. The range is inclusive.
7. To remove an entry, select the entry and click *Delete*.

3.8 Decoder Parameters

Some protocol decoders have user-defined parameters. These are protocols where some information cannot be discovered by looking at the data and must be entered by the user in order for the decoder to correctly decode the data. For example, such information might be a field where the length is either 3 or 4 bytes, and which length is being used is a system option.

If you have decoders loaded which require decoder parameters, a window with one tab for every decoder that requires parameters appears the first time the decoder is loaded.

For help on setting the parameters, click the Help button on each tab to get help information specific to that decoder.

If you need to change the parameters later,

- Choose Set Initial Decoder Parameters from the Options menu on the Control, Frame Display or Protocol Navigator windows.

- Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The Set Subsequent Decoder Parameters dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter

- Select the frame where the change should take effect
- Select Set Subsequent Decoder Parameters from the Options menu, and make the needed changes.
- Each entry in the Set Subsequent Decoder Parameters dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

3.8.1 A2DP Decoder Parameters

3.8.1.1 Selecting A2DP Decoder Parameters

The decoding of SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame in detail. You can increase the decoding speed by decoding only the header fields and not all the parts if they are not required. You can select the detail-level of decoding using the **Set Initial Decoder Parameters** dialog.

Note: By default the decoder decodes only the header fields of the frame.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *A2DP* tab.
3. Choose the desired decoding method.
4. Click the *OK* button to apply the selection and exit the *Set Initial Decoder Parameters* dialog.

3.8.2 Security Parameters

3.8.2.1 Security Key

On the Set Initial Decoder Parameters dialog, the security tab allows specifying a key for software decryption of 802.11 frames. One can enter two types of keys. The types are a WPA (Wi-Fi Protected Access) pre-shared key and a WEP (Wired Equivalent Privacy) key.

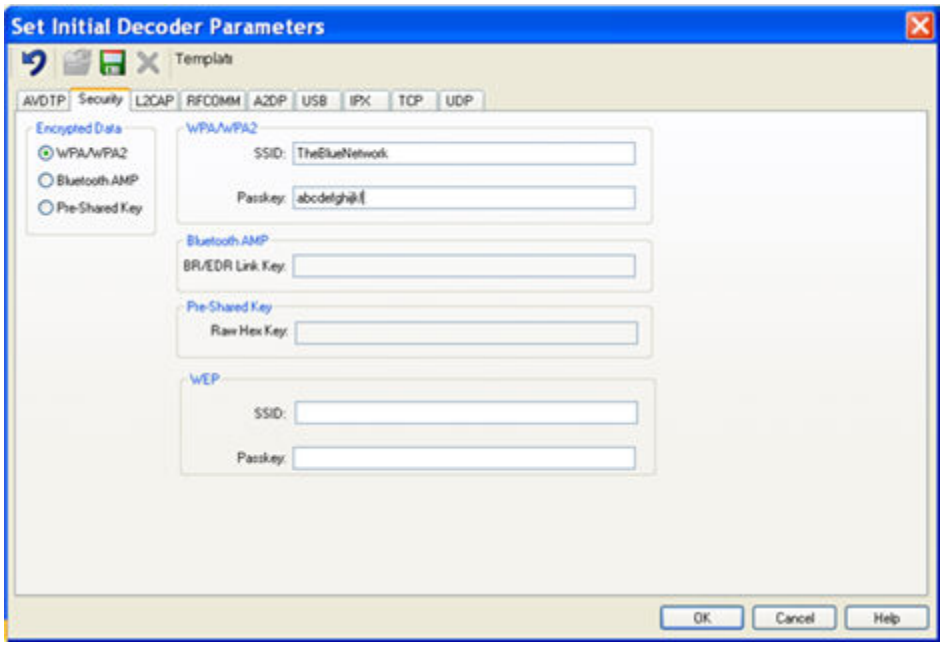
To access this dialog:

1. Go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters.*
2. Select the *Security* tab.

There are three types of types of encrypted data on the security tab, each one selectable via a radio button.

- WPA, WPA2 (Wi-Fi Protected Access), and WEP (Wired Equivalent Privacy) data that is transmitted over a Wi-Fi communications link. There are two values you have to enter for the WPA/WPA2 and WEP to be decrypted properly.
- The Bluetooth® alternative MAC/PHY (AMP) enables Bluetooth to support data rates up to 24Mbps by using additional wireless radio technologies.
- The Pre-Shared Key: The third way is to specify the pre-shared key in its raw hex forum. This is a 32 byte hex number.
  Note: When you use WPA/WPA2, the Pre-Shared key is generated automatically.

Depending on which Encrypted Data type you select, the options for entering data on the rest of the dialog varies.



3.8.3 AVDTP Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The dialog allows the user to define any number of parameters and save them in a Parameter Template for later use.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. The AVDTP Set Initial Decoder Parameters dialog requires the following user inputs to complete a Parameter:

- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Device Role
  This identifies the role of the device initiating the frame (master or slave)
- L2CAP Channel
  The channel number 0 through 78
- AVDTP Carries
  Select the protocol that AVDTP traverses to from the following:
  - AVDTP Signaling
  - AVDTP Media
  - AVDTP Reporting
  - AVDTP Recovery
  - -Raw Data-

3.8.3.1 Selecting and Applying an AVDTP Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *AVDTP* tab
   The dialog displays the content of the most recently selected Parameter Template in the

Initial Connections list at the top of the tab. If the template displayed is the desired template, then skip to step 4. If it is not, then continue with step 3.

3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.8.3.2 AVDTP Parameters

3.8.3.2.1 ADDING AN AVDTP PARAMETER

This procedure adds one or more parameters to an existing Parameter Template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File button and select the desired template from the Popup list.
3. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
4. Select the Device Role.
   This identifies the role of the device initiating the frame (master or slave)
5. Enter the L2CAP Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.
6. Select the protocol AVDTP Carries.
   Select the protocol that AVDTP traverses to from the list
7. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.
8. Click the Save icon at the top of the dialog to display the *Save As* dialog.

9. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template

10. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

11. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.3.2.2 DELETING AN AVDTP PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected Parameter Template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the *Set Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.3.3 AVDTP Parameter Templates

3.8.3.3.1 ADDING AN AVDTP PARAMETER TEMPLATE

This procedure adds a Parameter Template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *AVDTP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults button at the top of the dialog to clear the *Initial Connections* list.

4. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

5. Select the Device Role.
   This identifies the role of the device initiating the frame (master or slave).

6. Enter the L2CAP Channel
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

7. Select the AVDTP Carries
   Select the protocol that AVDTP traverses to from the list.

8. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

9. Click the Save button at the top of the dialog to display the *Save As* dialog.

10. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

11. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.3.3.2 DELETING AN AVDTP PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *AVDTP* tab
   The dialog displays the most recently selected Parameter Template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete button at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.8.3.4 AVDTP Missing Decode Information

3.8.3.4.1 AVDTP MISSING DECODE INFORMATION

The analyzer usually determines the protocol carried in an AVDTP payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the AVDTP payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.8.3.5 AVDTP Override Decode Information

3.8.3.5.1 AVDTP OVERRIDE DECODE INFORMATION

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click *OK*.

Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.8.4 L2CAP Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame but did not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in a Parameter Template for later use. To access this dialog:

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

For more on setting parameters, see Selecting and Applying an L2CAP Parameter Template.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The L2CAP Set Initial Decoder Parameters dialog requires the following user inputs to complete a Parameter :

- Stream
  This identifies the role of the device initiating the frame (master or slave)
- Channel ID
  The channel number 0 through 78
- Connection Handle
  This is the actual physical connection values for the devices
- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Carries (PSM)
  Select the protocol that L2CAP traverses to from the following:
  - AMP Manager
  - AMP Test Manager
  - SDP
  - RFCOMM
  - TCS
  - LPMP
  - BNEP
  - HCRP Control
  - HCRP Data
  - HID
  - AVCTP
  - AVDTP
  - CMTP
  - MCAP Control
  - IEEE P11073 20601
  - -Raw Data-

3.8.4.1 Selecting and Applying an L2CAP Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab
   The dialog displays the content of the most recently selected Parameter Template in the *Initial Connections* list at the top of the tab. If the template displayed is the desired template , then skip to step 4. If it is not, then continue with step 3.

3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.8.4.2 L2CAP Parameters

3.8.4.2.1 ADDING AN L2CAP PARAMETER

This procedure adds one or more parameters to an existing Parameter Template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window  , the Frame Display window  , or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File icon and select the desired template from the Popup list.
3. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).
4. Enter the Channel ID.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.
5. Enter the Connection Handle.
   This is the L2CAP address.
6. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.
7. Select the Carries (PSM).
   Select the protocol that L2CAP traverses to from the list.
8. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.
9. Click the Save icon at the top of the dialog to display the *Save As* dialog.
10. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
    The system displays a dialog asking for confirmation of the change to the existing template.

11. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.4.2.2 DELETING AN L2CAP PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected Parameter Template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the *Set Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.4.3 L2CAP Parameter Templates

3.8.4.3.1 ADDING AN L2CAP PARAMETER TEMPLATE

This procedure adds a Parameter Template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *L2CAP* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

5. Enter the Channel ID.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

6. Enter the Connection Handle.
   This is the L2CAP address.

7. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

8. Select the Carries (PSM).
   Select the protocol that L2CAP traverses to from the list.

9. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

10. Click the Save icon at the top of the dialog to display the *Save As* dialog.

11. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.4.3.2 DELETING AN L2CAP PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *L2CAP* tab
   The dialog displays the most recently selected Parameter Template content in the *Initial Connections* list at the top of the tab.

3. Click the Delete button at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.8.4.4 L2CAP Missing Decode Information

FTS4BT usually determines the protocol carried in an L2CAP payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the L2CAP payload of this frame (and other frames with the same LT_ADDR and CID that originate from the same side) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

Most often, the first L2CAP session in a connection is for SDP. If the data you are looking at seems to be in the first connection, selecting SDP in the dialog may yield useful results.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.8.4.5 L2CAP Override Decode Information

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Then choose the protocol the selected item carries from the drop-down list, and click *OK*.
5. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.8.5 RFCOMM Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in Parameter Templates for later use.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

For more on setting parameters, see Selecting and Applying an RFCOMM Parameter Template.

The Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each *Bluetooth*® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The RFCOMM Set Initial Decoder Parameters dialog requires the following user inputs to complete a parameter:

- Stream
  This identifies the role of the device initiating the frame (master or slave)
- Server Channel
  The channel number 0 through 78

- DLCI
  This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server
- Data Source Number
  When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- Carries (UUID)
  Select from the list to apply the Universal Unique Identifier (UUID) of the application layer that RFCOMM traverses to from the following:
  - OBEX
  - SPP
  - encap asyncPPP
  - Headset
  - FAX
  - Hands Free
  - SIM Access
  - VCP
  - UDI
  - -Raw Data-

3.8.5.1 Selecting and Applying an RFCOMM Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab
   The dialog displays the content of the most recently selected template in the *Initial Connections* list at the top of the tab. If the template displayed is the desired Connection Set , then skip to step 4. If it is not, then continue with step 3.
3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exits the *Set Initial Decoder Parameters* dialog.

3.8.5.2 RFCOMM Parameters

3.8.5.2.1 ADDING AN RFCOMM PARAMETER

This procedure adds one or more parameters to an existing template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template , then click the Open File icon and select the desired template from the Popup list.

3. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

4. Enter the Server Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

5. Enter the DLCI.
   This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server.

6. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

7. Select the Carries (UUID).
   Select the application layer that RFCOMM traverses to from the list to apply the Universal Unique Identifier for the necessary application layer.

8. Click the Add button.
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 8 until all desired parameters are added.

9. Click the Save icon at the top of the dialog to display the *Save As* dialog.

10. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
    The system displays a dialog asking for confirmation of the change to the existing template.

11. Click the *Yes* button.
    The system saves the new parameter to the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.5.2.2 DELETING AN RFCOMM PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the *Set Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.5.3 RFCOMM Parameter Templates

3.8.5.3.1 ADDING AN RFCOMM PARAMETER TEMPLATE

This procedure adds a template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Select the Stream.
   This identifies the role of the device initiating the frame (master or slave).

5. Enter the Server Channel.
   Enter the channel number 0 through 78, it can be entered as a decimal or a hexadecimal.

6. Enter the DLCI.
   This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server.

7. Enter the Data Source Number.
   When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source.

8. Select the Carries (UUID).
   Select the application layer that RFCOMM traverses to from the list to apply the Universal Unique Identifier for the necessary application layer.

9. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 9 until all desired parameters are added.

10. Click the Save icon at the top of the dialog to display the *Save As* dialog.

11. Enter a name for the new template and click *Ok*.
    The system saves the template and closes the *Save As* dialog.

12. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.5.3.2 DELETING AN RFCOMM PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *RFCOMM* tab
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete icon at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.

4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.8.5.4 RFCOMM Missing Decode Information

3.8.5.4.1 RFCOMM MISSING DECODE INFORMATION

FTS4BT usually determines the protocol carried in an RFCOMM payload by monitoring previous traffic. However, when this fails to occur, the Missing Decoding Information Detected dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- The capture session started after transmission of the vital information
- The analyzer incorrectly received a frame with the traversal information
- The communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the RFCOMM payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.8.5.5 RFCOMM Override Decode Information

3.8.5.5.1 RFCOMM OVERRIDE DECODE INFORMATION

The Set *Subsequent Decoder Parameters* dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect, and select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
2. Select the rule you wish to modify from the list of rules.
3. Choose the protocol the selected item carries from the drop-down list, and click *OK*.
4. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.8.6 ROC Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in Parameter Templates for later use.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

For more on setting parameters, see Selecting and Applying a ROC Parameter Template.

The Parameter Template function provides the capacity to create multiple Parameter Templates that contain different parameters. This capability allows the user to maintain individual Parameter Templates for each Remote Operations Controller (ROC) network monitored. Applying a Parameter Template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The ROC Set Initial Decoder Parameters dialog requires the following user inputs to complete a parameters:

- Device Address
  Complete the following fields to identify the device address:
  - Unit
    The 1-byte unit code of the individual device
  - Group
    The 1-byte group code of the group that contains the individual device identified in the "Unit" field

- Device Type
  Select the device type from the following:
  - FlashPAC
  - FloBoss 2xx
  - FloBoss 407
  - FloBoss 503
  - FloBoss504
  - RegFlo 2xx
  - ROC 809
  - ROCPAC

Sort and order the parameters list using the Sort Order and Sort Direction drop down fields at the top of the dialog.

3.8.6.1 Selecting and Applying a ROC Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *ROC* tab
   The dialog displays the content of the most recently selected Parameter template in the list at the bottom of the tab. If the Parameter Template displayed is the desired Parameter Template , then skip to step 4. If it is not, then continue with step 3.
3. Click the Open File icon at the top of the dialog and select the desired Parameter Template from the Popup list.
   The system displays the content of the selected Parameter Template in the list at the bottom of the dialog.
4. Click the *OK* button to apply the selected Parameter Template and exit the *Set Initial Decoder Parameters* dialog.

3.8.6.2 ROC Parameters

3.8.6.2.1 ADDING AN ROC PARAMETER

This procedure adds one or more parameters to an existing Parameter Template. To create a new Parameter Template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *ROC* tab.
   The dialog displays the most recently selected Parameter Template content in the list at the bottom of the tab. If the parameter must reside in another Parameter Template, then click the Open File icon and select the desired Parameter Template from the Popup list.

3. Enter the Device Address as follows:
   - Enter the 1-byte unit code of the individual device in the Unit field
   - Enter the 1-byte group code of the group that contains the individual device identified in the "Unit" field in the Group field
   - Select the Device Type from the list

4. Click the Add button

   The system displays the new parameter in the list. Repeat steps 3 and 4 until all desired parameters are added.

5. Click the Save icon at the top of the dialog to display the *Save As* dialog.

6. Ensure that the name of the Parameter Template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing Parameter Template.

7. Click the *Yes* button.
   The system saves the new parameter to the Parameter Template and closes the *Save As* dialog.

8. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the Parameter Template and close the dialog.

3.8.6.2.2 DELETING A ROC PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *ROC* tab.
   The dialog displays the most recently selected Parameter Template content in the list at the bottom of the tab. If the Parameter marked for deletion resides in another Parameter Template, then click the Open File icon and select the desired Parameter Template from the Popup list.

3. Select (click on and highlight) the Parameter marked for deletion from the *Initial Connection* list and click the Delete button above the list
   The system removes the selected Parameter from the list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the Parameter Template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing Parameter Template.
6. Click the *Yes* button.
   The system saves the Parameter Template and closes the *Save As* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the Parameter Template and close the dialog.

3.8.6.2.3 EDITING A ROC PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *ROC* tab.
   The dialog displays the most recently selected Parameter Template content in the list at the bottom of the tab. If the Parameter marked for edit resides in another Parameter Template, then click the Open File icon and select the desired Parameter Template from the Popup list.
3. Double click to select the Parameter marked for edit from the list
   Double clicking the Connection Statement populates the edit fields.
4. Edit the values in the fields as needed.
5. Click the Modify button above the list
6. Click the Save icon at the top of the dialog to display the *Save As* dialog.
7. Ensure that the name of the Parameter Template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing Parameter Template.
8. Click the *Yes* button.
   The system saves the new Parameter to the Parameter Template and closes the *Save As* dialog.
9. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the Parameter Template and close the dialog.

3.8.6.3 ROC Parameter Templates

3.8.6.3.1 ADDING A ROC PARAMETER TEMPLATE

This procedure adds a Parameter Template to the system and saves it for later use. A Parameter Template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing Parameter Template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *ROC* tab.
   The dialog displays the most recently selected Parameter Template content in the list at the bottom of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the list.

4. Enter the Device Address as follows:

   * Enter the 1-byte unit code of the individual device in the Unit field

   * Enter the 1-byte group code of the group that contains the individual device identified in the "Unit" field in the Group field

   * Select the Device Type from the list

5. Click the Add button
   The system displays the new parameter in the list at the bottom of the tab. Repeat steps 4 and 5 until all desired parameters are added.

6. Click the Save icon at the top of the dialog to display the *Save As* dialog.

7. Enter a name for the new Parameter Template and click *Ok*.
   The system saves the Parameter Template and closes the *Save As* dialog.

8. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the Parameter Template and close the dialog.

3.8.6.3.2 DELETING A ROC PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *ROC* tab
   The dialog displays the most recently selected Parameter Template content in the list at the bottom of the tab.
3. Click the Delete icon at the top of the dialog.
   The system displays *Delete* dialog with a list of saved Parameter Templates.
4. Select (click on and highlight) the Parameter Template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected Parameter Template from the list of saved Parameter Templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.8.7 USB Decoder Parameters

There may be times when the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame, then the decode for the response may be incomplete. The Set Initial Decoder Parameters dialog provides a means to supply the context for any frame. The system allows the user to define any number of parameters and save them in templates for later use.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.

The USB Template function provides the capacity to create multiple templates that contain different parameters. This capability allows the user to maintain individual templates for each USB network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. The USB Set Initial Decoder Parameters dialog requires the following user inputs to complete a parameter:

- Function Address (Range: 1-127)
  This is the decimal address of the USB port that connects the device to the computer.
- End Point Address (Range: 1-15)
  This is the decimal address of the operation within the device.
- USB Carrying
  Select from the list to apply the USB application

3.8.7.1 Selecting and Applying a USB Parameter Template

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab
   The dialog displays the content of the most recently selected template in the *Initial Connections* list at the top of the tab. If the template displayed is the desired template, then skip step 3 and go to step 4. If it is not, then continue with step 3.
3. Click the Open File icon at the top of the dialog and select the desired template from the Popup list.
   The system displays the content of the selected template in the *Initial Connections* list at the top of the dialog.
4. Click the *OK* button to apply the selected template and exit the *Set Initial Decoder Parameters* dialog.

3.8.7.2 USB Parameters

3.8.7.2.1 ADDING A USB PARAMETER

This procedure adds one or more parameters to an existing template. To create a new template, see Adding a Parameter Template.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab. If the parameter must reside in another template, then click the Open File icon and select the desired template from the Popup list.
3. Enter the Function Address (Range: 1-127)
   This is the decimal address of the USB port that connects the device to the computer.

4. Enter the End Point Address (Range: 1-15)
   This is the decimal address of the operation within the device.

5. Select the USB Application from the list of applications.

6. Click the Add button
   The system displays the new parameter in the *Initial Connection* window. Repeat steps 3 through 6 until all desired parameters are added.

7. Click the Save icon at the top of the dialog to display the *Save As* dialog.

8. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.

9. Click the *Yes* button.
   The system saves the new parameter to the template and closes the *Save As* dialog.

10. Click the *Ok* button on the S*et Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.7.2.2 DELETING A USB PARAMETER

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connection* list at the top of the tab. If the parameter marked for deletion resides in another template, then click the Open File icon and select the desired template from the Popup list.
3. Select (click on and highlight) the parameter marked for deletion from the *Initial Connection* list and click the Delete button at the bottom of the S*et Initial Decoder Parameters* dialog.
   The system removes the selected parameter from the *Initial Connection* list.
4. Click the Save icon at the top of the dialog to display the *Save As* dialog.
5. Ensure that the name of the template is listed in the *Save As* text box and click *Ok*.
   The system displays a dialog asking for confirmation of the change to the existing template.
6. Click the *Yes* button.
   The system saves the template and closes the *Save As* dialog.

7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.7.3 USB Parameter Templates

3.8.7.3.1 ADDING A USB PARAMETER TEMPLATE

This procedure adds a template to the system and saves it for later use. A template is a collection of parameters required to completely decode communications between multiple devices. To add a parameter to an existing template, see Adding a Parameter.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.

2. Click on the *USB* tab.
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.

3. Click the Reset to Defaults icon at the top of the dialog to clear the *Initial Connections* list.

4. Enter the Function Address (Range: 1-127).
   This is the decimal address of the USB port that connects the device to the computer.

5. Enter the End Point Address (Range: 1-15).
   This is the decimal address of the operation within the device.

6. Select the USB Application from the USB Carrying drop-down list.

7. Click the Add button.
   The system displays the new parameter in the *Initial Connections* window. Repeat steps 4 through 7 until all desired parameters are added.

8. Click the Save icon at the top of the dialog to display the *Save As* dialog.

9. Enter a name for the new template and click *Ok*.
   The system saves the template and closes the *Save As* dialog.

10. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the template and close the dialog.

3.8.7.3.2 DELETING A USB PARAMETER TEMPLATE

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control  window, the Frame Display  window, or the Protocol Navigator  window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *USB* tab
   The dialog displays the most recently selected template content in the *Initial Connections* list at the top of the tab.
3. Click the Delete icon at the top of the dialog.
   The system displays the *Delete* dialog with a list of saved templates.
4. Select (click on and highlight) the template marked for deletion and click the Delete button on the *Delete* dialog.
5. The system removes the selected template from the list of saved templates.
6. Click the *Ok* button on the *Delete* dialog to complete the deletion process and close the *Delete* dialog.
7. Click the *Ok* button on the *Set Initial Decoder Parameters* dialog to apply the deletion and close the dialog.

3.8.7.4 USB Missing Decode Information

The system usually determines the protocol carried in an USB payload by monitoring previous traffic. However, when this fails to occur, the *Missing Decoding Information Detected* dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- the capture session started after transmission of the vital information
- the analyzer incorrectly received a frame with the traversal information
- the communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the USB payload of this frame (and other frames with the same address) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under “data” in the detail pane on the frame display. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.8.7.5 USB Override Decode Information

The Set *Subsequent Decoder Parameters* is a selection from the Options menu on the Frame Displays dialog. This option allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter :

1. Select the frame where the change should take effect.
2. Select *Set Subsequent Decoder Parameters* from the *Options* menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click *OK*.
5. Each entry in the *Set Subsequent Decoder Parameters* dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.8.8 Decoder Parameter Templates

3.8.8.1 Adding a New or Saving an Existing Template

A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Enter a name for the new template and click Ok.

The system saves the template and closes the Save As dialog.

3. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

Save Changes to a Template

This procedure saves changes to parameters in an existing template.

1. After making changes to parameter settings in a user defined template, click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Ensure that the name of the template is listed in the Save As text box and click Ok.

The system displays a dialog asking for confirmation of the change to the existing template.

3. Click the Yes button.

The system saves the parameter changes to the template and closes the Save As dialog.

4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

3.8.8.2 Deleting a Template

1. After opening the *Set Initial Decoder Parameters* dialog click the Delete button at the top of the dialog.

   The system displays the Delete dialog with a list of saved templates.

2. Select (click on and highlight) the template marked for deletion and click the Delete button on the Delete dialog.

   The system removes the selected template from the list of saved templates.

3. Click the Ok button on the Delete dialog to complete the deletion process and close the Delete dialog.
4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the deletion and close the dialog.

3.9 Spy Mode

Spy Mode lets you run the analyzer on a computer, and "spy" on the data going in and out of a COM port or internal modem. This means that you can run both the analyzer and a communications application on the same computer, and use the analyzer to monitor the conversation between the application and another device. Since internal modems look like COM ports to the computer, the analyzer can monitor data passing through an internal modem as well as a regular COM port.

There are some limitations on using Spy Mode. the analyzer uses a custom version of the standard serial device driver in order to "spy" on COM ports and internal modems. This means that the analyzer must be started before the communications application to ensure that the analyzer's driver is being used by both the analyzer and the application. As a corollary, the port you are monitoring must normally use the standard serial driver, and not a custom driver.

To enter Spy Mode, you must follow the steps below in the order given.

1. Start the analyzer. The analyzer must be started before the application you are monitoring is started, or the application does not use the correct driver and the analyzer is not able to monitor the port.

2. From the Options menu on the Control window, choose Hardware Settings.
3. Click on the radio button labeled *Spy*.
4. Select the COM port you want to monitor.
5. Exit the Hardware Settings window.
6. Start the application. Be sure to have the application use the same COM port as the one chosen for the analyzer.
7. Monitor data.
8. Close your application when finished. If you want to monitor another application, repeat steps 6 - 8.
9. Close the analyzer.

It is important to follow the steps in the order given because this ensures that the analyzer's driver is the one being used by the application you are monitoring. Please note that the analyzer's driver is designed to behave like the standard serial driver when used by any other application. However, because it is not the standard serial driver, total compatibility cannot be guaranteed. See The FTS Serial Driver for more information.

The use of FIFO buffers may cause incorrectly sequenced data when in Spy Mode. See FIFOs and Spy Mode for more information.

3.9.1 Spy Mode Settings on the I/O Settings Dialog

Most of the settings on the I/O Settings window are grayed out in Spy mode because they are determined by the application using the COM port.

The analyzer updates these settings to reflect changes made by the application, allowing you to see the actual settings being used by the application.

If you are monitoring framed data, you need to choose a protocol stack in order to ensure that the data is framed correctly. You can also choose whether to monitor both sides of the circuit, or just the DTE or DCE side.

You also have the option of choosing to monitor all incoming data, regardless of whether the application you are monitoring is running.

You can also choose to monitor only when the application has opened the COM port and is actively communicating through the port. By default, the analyzer monitors all data, all the time, which means that the analyzer may show captured data before you have opened your application. To monitor the port only when the application has opened it, check the *Capture Only When Spied Port is Open* box on the *I/O Settings* dialog.

3.9.2 FIFOs and Spy

The 8250 UART generates an interrupt every time a byte enters the UART. If the UART is receiving data at a high rate of speed, it generates frequent interrupts which the central processor has to deal with, leaving the central processor less time for other tasks. If the

central processor cannot retrieve the bytes quickly enough, data is lost as new data overwrites the information stored in the UART. The solution to this problem was the development of new UART chips that had buffers.

The 16550 UART, one of the most common UARTs currently in use, has a 16 byte buffer. The buffer operates on the First In, First Out (FIFO) principle. The first byte in the buffer is the first byte to go out of the buffer. The buffer allows the UART to store bytes until a specified number of bytes have come in, at which point it generates an interrupt telling the central processor to retrieve the data. The ability to store bytes means that the UART is not generating as many interrupts, giving the central processor more time for other tasks.

There are two problems with the buffering system and Spy mode. One is that data may not be timestamped accurately, and the other is that control signal states may not be correct. the analyzer timestamps the byte and records the state of the control signals at the time it retrieves the byte from the UART. If the buffers are being used, an interrupt is generated until several bytes have already come in, possibly resulting in incorrect timestamps and signal states.

The analyzer solves the problem by telling the UART to generate an interrupt every time a byte comes in, but the analyzer cannot do this when operating in Spy mode. In Spy mode, the application being monitored has control of the UART and specifies how the buffers is used. The result is that the captured data may not be completely accurate.

If you are using Spy mode, we recommend turning off the FIFOs on the UART if accurate recording of timestamps or control signal states is important.

3.9.3 Turning Off the FIFO Buffers

In Windows XP

1. Click on the *Start* button and choose *Control Panel*.
2. Click on the *Performance and Maintenance* selection, then the *System* selection.
   OR:
   Simply right click the *My Computer* icon on your desktop and select *Properties* from the Popup menu.
3. On the *System Properties* dialog, click on the *Hardware* tab, then click the *Device Manager* button.
4. Expand the *Ports* section, and double-click on the port you want to change to open the *Port Properties*.
5. Click the *Port Settings* tab on the *Communications Port Properties* dialog, followed by the *Advanced* button.
6. Un-check the box labeled *Use FIFO buffers* (requires 16550 compatible UART).
7. Click *OK* on all windows to close the windows.
8. Follow this same process to turn the FIFOs back on.

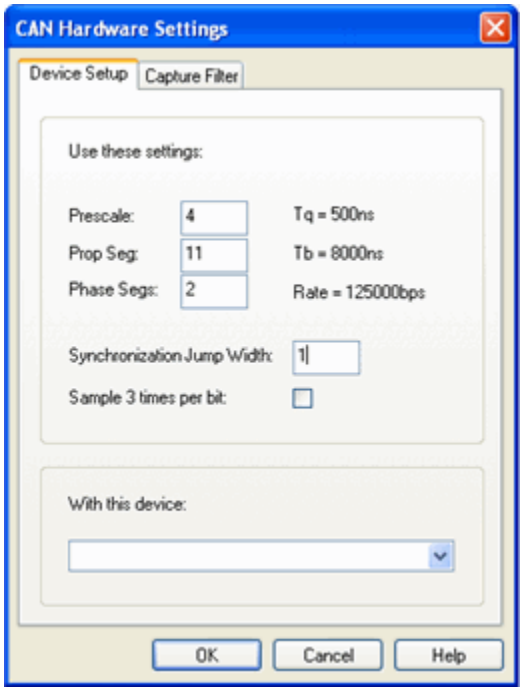
3.10 CAN 2.0A Special Instructions

3.10.1 CAN 2.0A Hardware Settings

Note:You must complete the SST Woodhead DeviceNet Card Installation before starting this procedure. You must setup your card before FTS can use it. This is done from the Hardware Settings window.

To setup the DeviceNet card:

1. Start NetDecoder and select CAN 2.0 from the Choose Protocol to Analyze dialog.
2. Then choose Hardware Settings from the Options menu on the Control window.
3. There are two tabs: Device Setup and Capture Filter. Choose Device Setup.



- **Prescale**

  This value is multiplied by the minimum time quantum of 125ns to produce the time quantum.

- **Prop Seg**

  This value is multiplied by the time quantum to produce the propagation time segment, which compensates for physical network delays.

- **Phase Seqs**
  This value is multiplied by the time quantum to produce phase buffer segment 1 and phase buffer segment 2, which may be lengthened or shortened to compensate for phase errors.
  The nominal bit time is the sum of the synchronization segment (one time quantum), propagation time segment, and phase buffer segments. The nominal bit rate is the inverse of the nominal bit time.

- **Synchronization Jump Width**
  Each bit is sampled at the end of phase buffer segment 1. The synchronization jump width is the number of time quanta by which phase buffer segment 1 is lengthened, or phase buffer segment 2 shortened, to resynchronize upon detection of a phase error.

- **Sample 3 times per bit**
  This enables two additional samples to be taken, one ahead of the normal sample point and one behind it, to eliminate detection of false bit values on noisy networks.

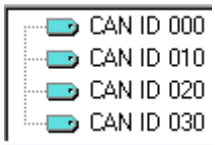
- **Device List**
  Select a capture device from the list of available devices found on your machine. If you are using an SST capture device, be sure to have the SST DeviceNet 32-bit Software installed; in addition to the device's basic drivers (see the section on Installing the SST Woodhead DeviceNet Card).

3.10.2 CAN 2/0A Capture Filters

You can define the Capture Filters on the Hardware Settings.

1. Start NetDecoder and select CAN 2.0 from the Choose Protocol to Analyze dialog.
2. Then choose Hardware Settings from the Options menu on the Control window.
3. There are two tabs: Device Setup and Capture Filter. Choose Capture Filter.

The Filter Panel displays the CAN IDs that is captured (or excluded) by the current filter.

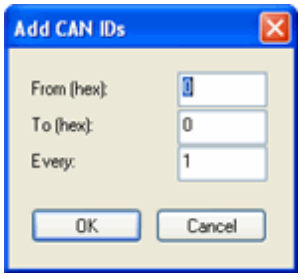


1. To create a filter, click the Add CAN ID button and add the CAN IDs you wish to filter on in the dialog box.
2. Click the Exclude check box to cause all CAN IDs except those listed in the filter panel to be captured.

3. Save the filter if desired. Click on the Save button and enter a file name.
4. Click OK. The filter is active when data capture is started.

3.10.2.1 Add/Remove CAN IDs Dialog

The Add/Remove CAN IDs dialog appears when you click the Add or Remove CAN ID buttons on the toolbar of the Capture Filter tab. This dialog is used to add (or remove) CAN IDs to/from a CAN Capture Filter.



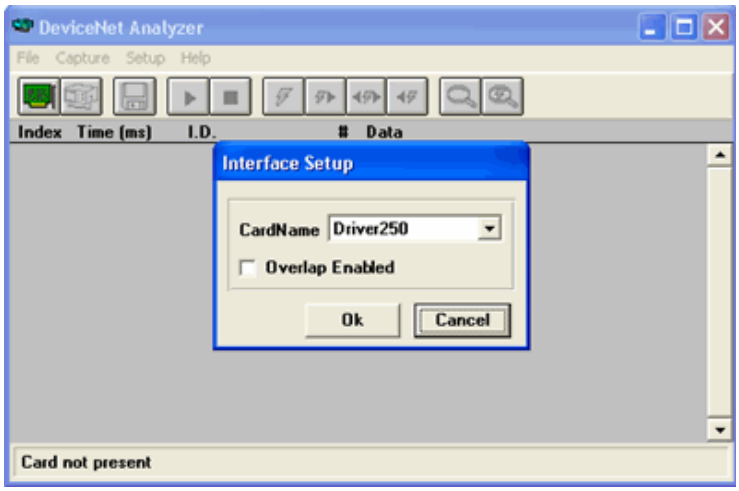
- **From** - A range of CAN IDs is specified starting at the From field. This value is edited in hexadecimal.
- **To** - A range of CAN IDs is specified up to and including the To field. This value is edited in hexadecimal.
- **Every** - The range specified includes only 'Every' n CAN IDs. This value is edited in decimal.

3.10.3 SST Woodhead DeviceNet Card Installation Instructions

The installation software on the CD is for Windows NT 4.0 with SP4, XP Pro, 2000 Pro, 2000 Server and Server 2003. We have also successfully installed the cards under XP Home Edition. If you need drivers for other operating systems, they can be downloaded from the SST Woodhead web site at http://www.woodhead.com.

1. Insert the SST DeviceNet software CD first, before inserting the card. The CD should auto run and display the main menu. If it does not, browse the CD and double-click on setup.exe.
2. Select Product Menu from the main menu.
3. Select your card type from the Product Menu screen.
4. Choose DeviceNet DNP Products Install 2.0 for NT/XP/2000/Server from the top drop-down list and click Next. Follow the installation instructions.

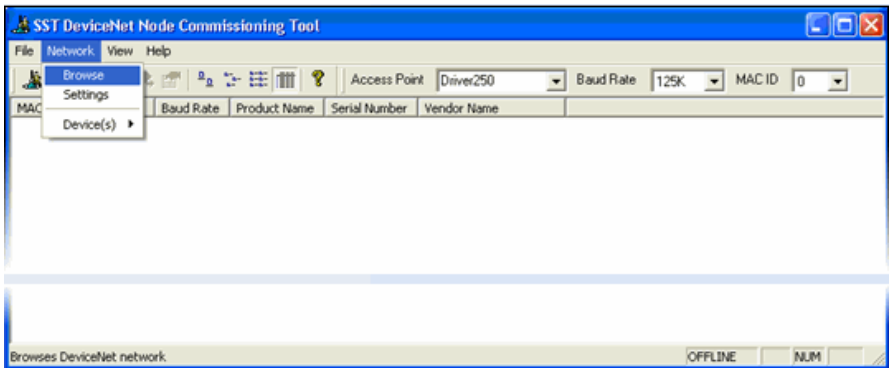
5. If you do not have an operational network: Go to Start | Programs | SST | DeviceNet DNP and select the DeviceNet Analyzer program.



Select the appropriate card name from the drop list. Once selected, notice that the health LED on the dongle turns green and the comm. LED reflects the communications status of the DeviceNet Network.

If you have an operational network:

Go to Start | Programs | SST | DeviceNet DNP and select the DeviceNet Commissioning Tool. Select the appropriate module from the Access Point drop list. If the module is functioning, the software allows you to browse the network for devices. Notice that the bottom of the window displays the status of the card and network.



3.11 ControlNet Special Instructions for the 1784-PCC

3.11.1 Capturing ControlNet Data

Before you begin, ensure that a 1784-PCC hardware interface card is connected to the analysis computer and that it is connected to the node you wish to monitor.

1. Start the analyzer and select ControlNet from the Choose Protocol to Analyze dialog.

2. (Optional) Choose *Hardware Settings* from the *Options* menu on the Control window and check the status of the 1784-PCC card.
3. Choose *I/O Settings* from the *Options* menu on the Control window and select the start and stop triggers or times, and capture filters to use.
4. Exit the I/O Settings dialog and start the analyzer.

Once the start trigger (or time) is detected, data capture begins and continues until the stop trigger (or time) is detected, or the buffer or file becomes full.

3.11.2 ControlNet Setup

3.11.2.1 ControlNet I/O Settings

Use the I/O Settings  dialog to select a buffer size, set and apply start and stop times or triggers to the capture session, and apply any capture filters to the data on the network. Selections made in the I/O Settings dialog are persistent during the analyzer session, but revert to the defaults when the analyzer is shutdown and re-started. The default settings are 32MB buffer size, no start or stop triggers selected, and no filters selected.

To Access the I/O Settings Dialog

1. Choose *I/O Settings* from the *Options* menu on the Control window.
2. Select a buffer size from the *BUFFER SIZE* list, or accept the default value.
3. If you want the capture to begin and end based on triggers, then select the start and stop triggers in the *START TRIGGERS* and *STOP TRIGGERS* panes by checking the boxes to the left of the trigger definitions.
   - If the triggers you want to use are not in the list, then you must define them. See Defining and Maintaining ControlNet Start and Stop Triggers
   - For more information on triggers see About Triggers
4. Select the filters you want to use in the *CAPTURE FILTERS* pane by checking the boxes to the left of the filter definitions.

   If the filters you want to use are not in the list, then you must define them. See Defining and Maintaining ControlNet Capture Filters
5. Click the *OK* button at the bottom of the I/O Settings dialog, and start the analyzer.

3.11.2.2 ControlNet Hardware Settings

The Hardware Settings display provides the current status of the installed 1784-PCC card in the following fields:

- Sniffer Hardware - Identifies the card currently installed. If this field is blank, then no card is installed.
- Memory Address - Identifies the dual-port memory address
- IRQ Number - Identifies the number of the protocol analyzer application
- Card Status - Indicates whether any application has "locked" the card
- Application Using the Card - If the card status is "Locked", then this indicates the application using the card.
- Firmware Version - Identifies the firmware version of the card

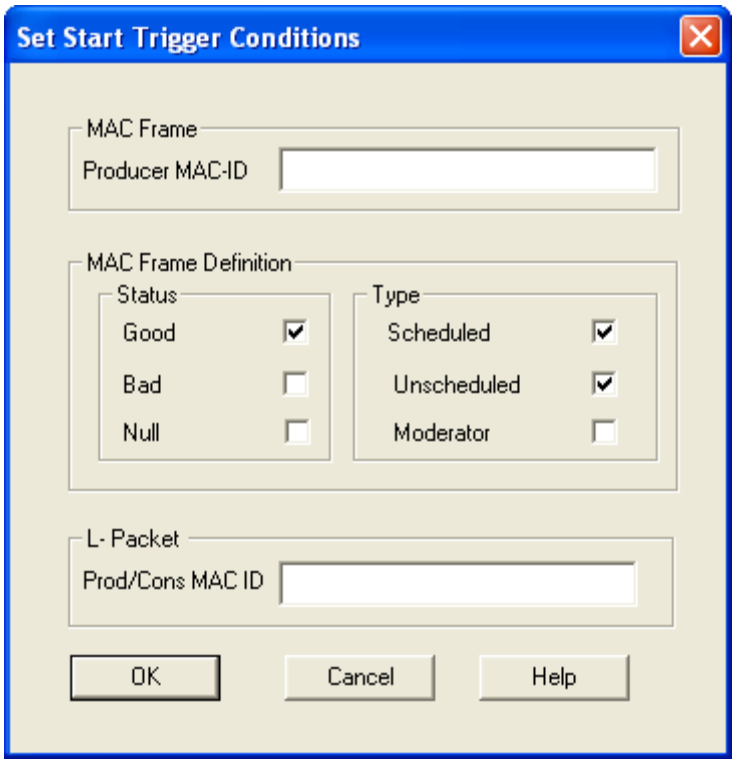
The 1784-PCC card is also used by other applications such as RSLinx. Only one application can have access to the 1784-PCC card at a time. When one of these applications is running, it locks the card and prevents other applications from accessing it.

3.11.2.3 Defining and Maintaining ControlNet Start and Stop Triggers

Start and Stop triggers are defined on the frame conditions.

See About Triggers for more information on making entries in the following dialogs.

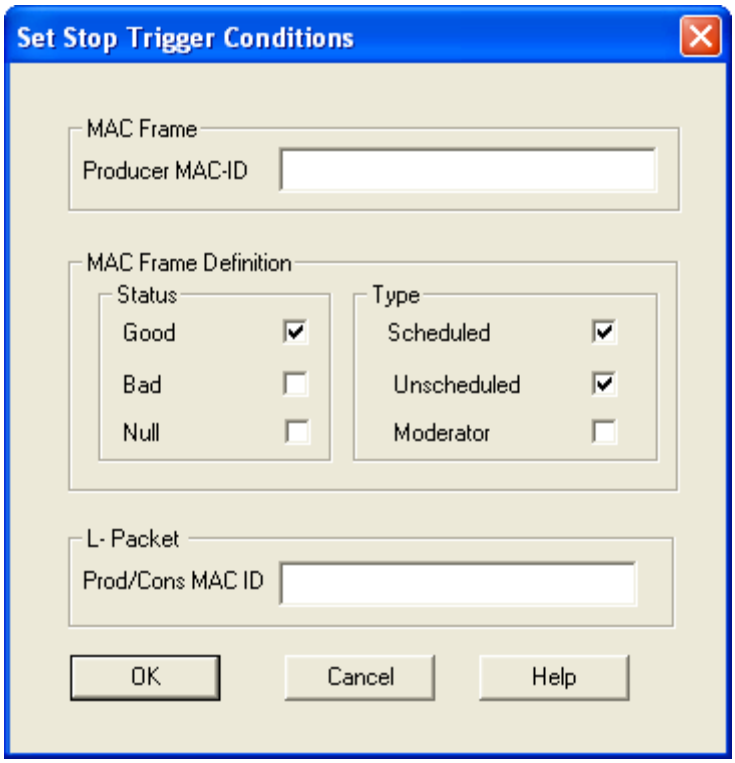
Defining a Start Trigger



1. Choose *I/O Settings* from the *Options* menu on the Control window.

2. Click on the *Add Start Conditions* button to display the *Set Start Trigger Conditions* dialog.
3. Enter the *Producer MAC ID* in the MAC Frame field. If you do not enter a value or values in this field, the full range (0-255) becomes the default value.
4. Select the Status in the MAC Frame Definition pane. One or more of these statuses may be selected, however at least one must be selected. Defaults to *Good* selected.
5. Select the Type in the MAC Frame Definition pane. One or more of these types may be selected, however at least one must be selected. Defaults to *Scheduled* and *Unscheduled* selected.
6. Enter the *Prod/Cons MAC ID* you want to trigger in each LPacket in the L-Packet field. If you do not enter a value or values in this field, the full range (0-255) becomes the default value.
7. Click the *OK button.*
8. The *Set Start Trigger Conditions* dialog closes and the new start trigger definition appears in the *START TRIGGERS* list on the I/O Settings dialog. This start trigger can now be selected and applied to the next capture session.

Defining a Stop Trigger



1. Choose *I/O Settings* from the *Options* menu on the Control window.
2. Click on the *Add* button to the right of the *STOP TRIGGERS* pane in the middle of the I/O Settings dialog to display the *Set Stop Trigger Conditions* dialog.
3. Enter the *Producer MAC ID* in the MAC Frame field. If you do not enter a value or values in this field, the full range (0-255) becomes the default value.
4. Select the Status in the MAC Frame Definition pane. One or more of these statuses may be selected, however at least one must be selected. Defaults to *Good* selected.

5. Select the Type in the MAC Frame Definition pane. One or more of these types may be selected, however at least one must be selected. Defaults to *Scheduled* and *Unscheduled* selected.
6. Enter the *Prod/Cons MAC ID* you want to trigger in each LPacket in the L-Packet field. If you do not enter a value or values in this field, the full range (0-255) becomes the default value.
7. Click the *OKI button.*
8. The *Set Stop Trigger Conditions* dialog closes and the new stop trigger definition appears in the *STOP TRIGGERS* list on the I/O Settings dialog. This stop trigger can now be selected and applied to the next capture session.

Editing Trigger Definitions

1. Choose *I/O Settings* from the *Options* menu on the Control window.
2. Highlight the trigger you want to change in the list pane.
3. Click the *Edit* button to the right of the list pane with the highlighted trigger definition.

The system displays the appropriate edit screen with the definition of the highlighted trigger.

4. Edit the fields you want to change and click the *OK* button.

Deleting Trigger Definitions

1. Choose *I/O Settings* from the *Options* menu on the Control window.
2. Highlight the trigger you want to change in the list pane.
3. Click the *Delete* button to the right of the list pane with the highlighted trigger definition.

The system deletes the highlighted trigger from the list.

3.11.2.4 Defining and Maintaining ControlNet Capture Filters

Capture filtering allows frames that meet a specified condition to pass from the network to the buffer. If the frame does not satisfy the filter criteria, it is thrown away. Data that is filtered out using a capture filter cannot be recovered. For example, you may set up a capture filter that only allows frames with a source MAC ID of 10 to pass from the network to the collection buffer. Frames from all source MAC IDs other than 10 are discarded.

After capturing frame data (filtered or unfiltered), the buffer or file can be filtered further by using a display filter. A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer or file and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Unlike a capture filter, where data that does not match is thrown away, all the data is kept when using a display filter. The filter just displays a subset of the data. Multiple display filters can be used simultaneously, and different windows can be displaying data using different filters.

3.11.2.5 About Triggers

Triggers:

Start and Stop triggers are defined on the frame conditions.

Start/Stop trigger on frame condition allow you to:

Define the Producer MAC ID(s) you want to trigger. You can define:

- a single Producer MAC ID (in a range 0-255).
- a group of IDs. Separate the range by a hyphen (2-88). The range can extended from 0 to 255.
- multiple IDs. Separate the IDs by a semi-colon (2;9;27).
- a group and multiple IDs (2-7;3;8).

  If you do not enter a value in this field, the full range (0-255) becomes the default value.

Define the Producer MAC ID(s) you want to trigger in each LPacket.

- For a Generic LPacket, it is the Producer/Consumer ID.
- For a Fixed LPacket, it is the Destination ID.
- For a Broadcast ID, it is 255.

  You can define:

- a single Producer/Consumer MAC ID (in a range 0-255).
- a group of IDs. Separate the range by a hyphen (2-88).

  The range can extended from 0 to 255.

- multiple IDs. Separate the IDs by a semi-colon (2;9;27).
- a group and multiple IDs (2-7;3;8).

Status of Frame

A frame status can be defined in three ways:

- Good: a frame correctly received by the Traffic Analyzer tool.
- Bad: the Traffic Analyzer tool has detected a problem with this frame (e.g. a CRC problem).
- Null: a frame without any data.

Type of Frame

A frame type can also be defined in three ways:

- Scheduled: Every scheduled node in sequential order is guaranteed one opportunity to transmit. Information that is time-critical is sent during the scheduled part of the interval. The bandwidth is reserved in advance to support real time data transfers. Real time data transfers include:
  - real time control data (I/O updates)

- analog data
- peer to peer interlocking

- Unscheduled: All nodes transmit on a rotating basis in sequential order. This rotation repeats until the time allocated for the unscheduled portion is used up. The amount of time available for the unscheduled portion is determined by the traffic load of the scheduled portion. ControlNet guarantees at least one node will have the opportunity to transmit unscheduled data every interval. The starting node for each NUT rotates to guarantee each node will have an unscheduled transmit time. The remaining bandwidth supports non time-critical data transfers. Non time-critical data transfers include:
  - connection establishment
  - peer to peer messaging
  - programming (uploads and downloads)
- Moderator: The node with the lowest MAC ID (node address) assumes the moderator role. The moderator frame is transmitted to keep the other nodes synchronized. This moderator frame is sent in the guardband.

3.11.2.6 Interpreting the Control Bytes Expanded Pane

The bits of the control field are numbered 0 through 7 and are described below.

- **Bit 0 - Fixed Tag (type of LPacket)**

  Bit 0 is the least significant bit of the control field. Bit 0 indicates the type of LPacket. When set (bit 0 = 1), the LPacket is a fixed tag LPacket. Conversely, when clear (bit 0 = 0), the LPacket is a generic tag LPacket.

- **Bit 1 - Tag Pad (Odd Tag Size)**

  Bit 1 of the control field indicates whether the tag field contains an even or odd number of bytes. When clear (bit 1 = 0), it indicates that the tag contains an even number of bytes. When set (bit 1 = 1), it indicates that the tag contains an odd number of bytes. A fixed LPacket has an even tag so bit 1 = 0 and a generic LPacket has an odd tag so bit 1 = 1.

- **Bit 2 - Data Pad (Odd Link Data Size)**

  Bit 2 of the control field indicates whether the link data contains an even or odd number of bytes. When clear (bit 2 = 0), it indicates that the link data contains an even number of bytes. When set (bit 2 = 1), it indicates that the link data contains an odd number of bytes.

- **Bit 3 - Reserved**

  Bit 3 of the control field is reserved.

- **Bit 4 - Generic Tag (Type of LPacket)**

  Bit 4 of the control field is the inverse of bit 0 (see bit 0 above). If bit 0 is clear, then bit 4 is set. If bit 0 is set, then bit 4 is clear.

- **Bit 5, 6, 7 - Reserved 7:5**

  Bits 5, 6, and 7 of the control field are reserved.

3.11.3 ControlNet Statistics

3.11.3.1 Network Monitoring

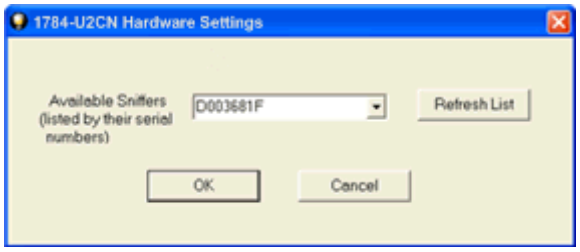
The network information corresponds to dynamic data collection over the ControlNet network. The following information is contained within the Network Information dialog box:

- Network Grid - displays the active nodes on the network.
- Network Attributes - the network attribute commands analyze the current moderator frames and display the following attributes:
  - Network Update Time (ms)
  - Scheduled Max. Node
  - Unscheduled Max. Node
  - Slot Time (ms)
  - Blanking Time
  - Guard Band Start (ms)
  - Guard Band Center (ms)
  - Guard Band Prestart (ms)
  - Interval Modulus (NUTs)
- Additional network information that does not come from the moderator. This information corresponds to Scheduled and Unscheduled elements, for which the following information is provided:
- Scheduled information in the Interval Modulus average bandwidth used and maximum bandwidth used
- Average available unscheduled information and average used unscheduled information in the Interval Modulus, both expressed in bytes per second

3.12 ControlNet Special Instructions for the 1784-U2CN

3.12.1 ControlNet 1784-U2CN Hardware Settings

The Hardware Settings dialog allows you to select a device to sniff/scan. You access the Hardware Settings dialog by selecting **Hardware Settings** from the **Options menu** on the NetDecoder Control window.



FTS automatically scans and identifies all the 1784-U2CN devices plugged into the PC. These devices, identified by their Serial Numbers, are displayed in the drop-down list of Available Sniffers.

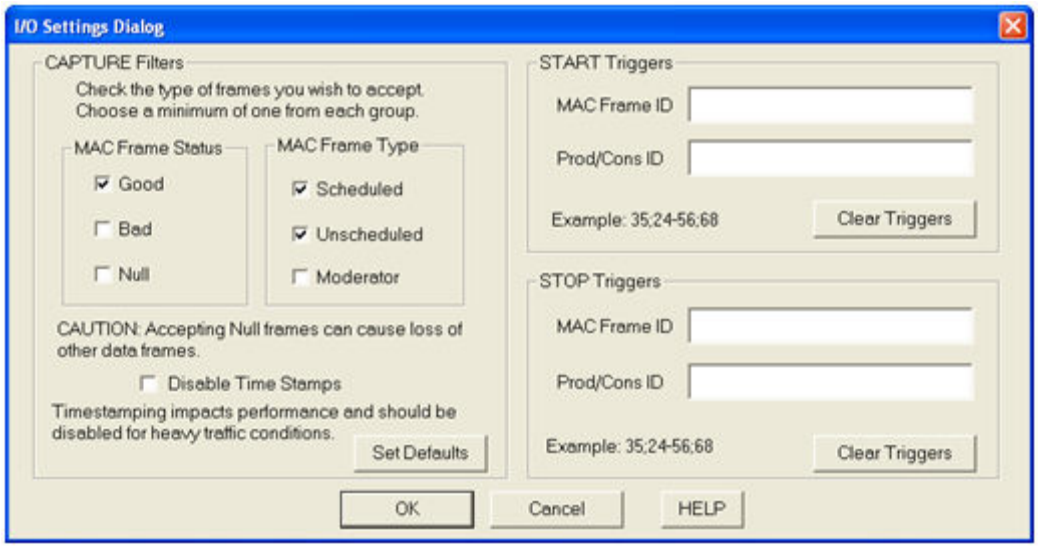
1. Select a device from the drop-down list
2. Select OK.

Selecting Cancel overrides all the selections and returns the user to the Control Window.

Note: You can select Refresh List to update the list of devices.

3.12.2 ControlNet 1784-U2CN I/O Settings

The ControlNet-U2CN Datasource I/O Settings Dialog provides the user options for setting **Capture Filters**, as well as **START** and **STOP** triggers.



Capture Filters

While capturing ControlNet traffic, the I/O Settings Dialog in the 1784-U2CN indicates the MAC Frame Status and the MAC Frame Type of each of the captured frames.

The Frame Status options are:

- Good
- Bad = erroneous data
- Null = empty frames

There are three types of frames on the network:

- Scheduled traffic
- Unscheduled traffic
- Frames sent by the Moderator.

You can choose to filter on ControlNet traffic based on the frame's status or type.

- You can select more than one from each group, but you must select at least **one MAC Frame Status** and **one MAC Frame Type**.
- The default setting for capture filters is **Good** for the Frame Status and **Scheduled** and **Uncheduled** for the Frame Type.

Disable Time Stamps

You can also choose to disable timestamps. When you activate **Disable Time Stamps**, the values in the place holders for the timestamps are random and the Frame Display will show incorrect values for the timestamps. You should ignore those values if timestamping is disabled.

START and STOP Triggers

A START trigger is defined as the event that starts data capture. The capture engine ignores all frames prior to the specified START trigger. All subsequent frames are captured until either a user-defined STOP trigger occurs or the user manually stops data capture.

A STOP trigger is defined as the event that stops data capture. The capture engine stops capturing all frames after the specified STOP trigger is reached.

You can define the START and STOP triggers according to the contents of the Source and Destination MAC IDs in the ControlNet frame.

- START and STOP triggers are applied after filtering data.
- The triggers are defined on the MAC ID of the frame or on the Prod/Cons ID.
- You can enter multiple individual IDs separated by a semi-colon. For example: “35;12;56;2”
- You can also a range of values. e.g. “12-28”
- You can also enter a combination of individual values and ranges. e.g.: “12;34;56-70;15”

3.13 Data Highway Plus Special Instructions

3.13.1 Data Highway Plus Setup for DL3500-DHM

The DL3500-DHM (Data Highway Monitor) adapter for use with NetDecoder is a special version of the product that was developed for Frontline Test Equipment, Inc. It includes firmware that allows the unit to promiscuously capture the data passing on a Data Highway Plus (DH+) network. The unit supports capturing data at 57.6K, 115.2K or 230.4Kbps. The DL3500-DHM hardware automatically senses the DH+ data rate and set the serial port interface to twice the DH+ rate. Apply power to the DL3500-DHM and then connect the network cable in order for the unit to automatically sense the network data rate.

There are two basic steps to beginning data capture:

- Connecting the DL3500-DHM hardware to the DH+ circuit and the PC running NetDecoder
- Configuring the I/O Settings in NetDecoder.

The following items are included with the DL3500-DHM:

- DL3500-DHM hardware
- Power supply
- 9-pin cable

You have to acquire a Blue Hose 3-wire cable.

CONNECTING THE DL3500-DHM

1. If you have not already done so, install the NetDecoder software and decoders on the PC you use to monitor the DH+ network.
2. Obtain a Blue Hose 3-wire cable. Attach one end of the Blue Hose to the DL3500-DHM's CHA Network interface and then attach the other end to the DH+ Port on one of the PLCs located on the DH+ network you wish to monitor.
3. Attach one end of the 9 pin cable supplied with the DL3500-DHM to the CHB/RS-232 interface on the DL3500-DHM and then attach the other end to a serial port on the PC you are running the NetDecoder software on.
4. Wire-up the power supply to the DL3500-DHM and plug it into a wall outlet.

CONFIGURING NETDECODER

1. If you have not already done so, connect the DL3500-DHM hardware.
2. Start NetDecoder and select from the Rockwell Allen Bradley folder.
3. Choose I/O Settings from the Window menu on the Control window, or click the I/O Settings icon to open the I/O Settings window.
4. In the Baud box, set the rate to twice the rate of the DH+ network. This is the rate at which data is received from the DL3500-DHM. The default value is 115.2K.

   a) In the DH+ Network box, set the rate to match the rate of the DH+ network. This network rate is used for calculation of some statistics in NetDecoder. The default value is 57.6K.

   b) See the online Help for information on the other settings in the I/O Settings window and how to save the configuration.

Now you are ready to capture data with NetDecoder! See the accompanying Quick Start Guide or the online Help to learn how to capture and review data using the NetDecoder software.

Changes to Header Bytes as a Result of Using the DL3500-DHM

The DL3500-DHM changes some of the data seen on the Data Highway Plus network in order to convert it to a form FTS can use.

First, the DL3500-DHM converts the data from synchronous to asynchronous. Second, it formats the frame as a DF1 full duplex with CRC message, which means it strips off 5 bytes from the original message and adds 6 DF1 bytes. A 0x1002 is placed at the beginning of the message, and a 0x1003, followed by two CRC bytes, is placed at the end. The CRC is an error check between the DL3000-DHM and FTS only, NOT an error check between any DH+ devices or the DH+ network and FTS.

3.13.2 Special Instructions for 1784-U2DHP

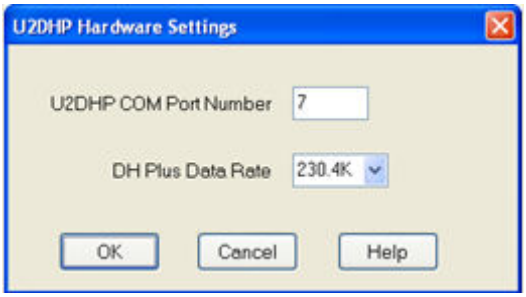
3.13.2.1 DH Plus 1784-U2DHP Hardware Settings

The 1784-U2DHP installs itself as a Serial COM Port on your PC. The Hardware Settings dialog allows you to set the COM Port number and the data rate that your device is using.

Also, before starting data capture with the 1784-U2DHP, you must:

- *Shut down RSLinx*
- *Set the correct COM Port number in this dialog.*

1. You access the Hardware Settings dialog by selecting **Hardware Settings** from the **Options menu** on the NetDecoder Control window.



There are two values you have to set: COM Port Number and Data Rate

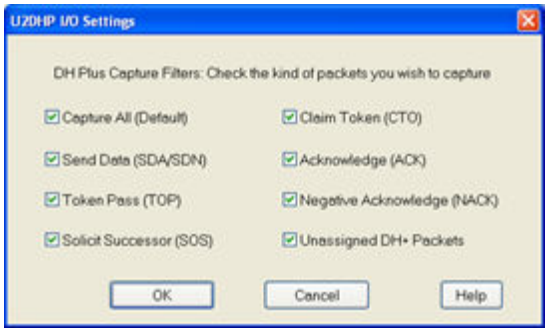
- To identify the COM port number, open your PC's Device Manager and look under the "Ports (COM & LPT)" section. Enter that number in this dialog. If the correct number is not set, then the data capture fails because NetDecoder will not be able to read the right data.
- DH+ can run at baud rates of 57.6K, 115.2K or 230.4K. The 1784-U2DHP has a knob to set the data rate. Make sure that the setting on your 1784-U2DHP matches your DH+ networks data rate. Then choose the right value in the drop down menu on the Hardware Settings dialog.

1. Enter the **COM Port** number.
2. Select a **data rate** from the drop-down list
3. Select **OK** to accept the values and close the dialog or **Cancel** to disregard the settings and close the dialog.

3.13.2.2 DH Plus 1784-U2DHP I/O Settings

The DH Plus analyzer, using the 1784-U2DHP, allows users to select what type of packets are captured. This type of filtering eliminates capturing unnecessary frames and allows the user to quickly pin-point the source of the network problem. You select which frames to capture using the I/O settings dialog.

You access the I/O Settings dialog by selecting **IO Settings** from the **Options menu** on the NetDecoder Control window.



1. Select the kind of DH+ frames you need to capture by clicking the appropriate check boxes.
   - If more than one box is checked, then the selection is treated as a logical AND condition.
   - The default setting is to capture all traffic.
   - If none of the items are checked on the dialog, the program defaults to a 'capture-all' state.

2. Select **OK** to accept the values and close the dialog or **Cancel** to disregard the settings and close the dialog.

3.14 DeviceNet Special Instructions for the SST Woodhead interface cards

3.14.1 DeviceNet I/O Settings

NOTE:

You must complete the SST Woodhead DeviceNet Card Installation before starting this procedure.

You must setup your card before FTS can use it. This is done from the I/O Settings window.

To setup the DeviceNet card:

1. Start NetDecoder and select DeviceNet from the Choose Protocol to Analyze dialog.
2. Then choose *I/O Settings* from the *Options* menu on the Control window.
3. There are two tabs: Device Setup and Capture Filter. Choose *Device Setup*.
4. Select the baud rate of the target network.
5. Select a capture device from the list of available devices found on your machine in the *With this device* box.

6. Select one, both, or neither of the capture option(s) from the two check boxes

Capture Options

- **Put interface offline in Bus Warning condition:** This is the default condition and will be checked when the dialog first appears. If a user starts a DeviceNet capture using the SST interface card with the wrong baud rate, the entire network could go offline. With this option, NetDecoder monitors the **Bus Warning** condition bit and once the bit exceeds the set limit, the card is put offline to protect the network.
- **Stop capture on Error condition:** This is a stop trigger that stops the capture whenever a error condition is detected on the bus.

Note: Both options can be selected or neither option has to be selected.

3.14.2 DeviceNet Capture Filters

1. Start NetDecoder and select DeviceNet from the Choose Protocol to Analyze dialog.
2. Then choose *I/O Settings* from the *Options* menu on the Control window.
3. There are two tabs: Device Setup and Capture Filter. Choose *Capture Filter*.

Toolbar Buttons

Creating a Filter

 Clears the current filter settings

 Loads a filter from disk

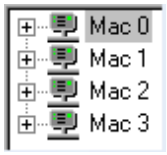
 Saves the current filter to disk

 Opens the Add Message dialog (information on this dialog follows bellow)

 Expands all nodes in the filter display

 Collapses all nodes in the filter display

The Filter Panel on the left displays the messages that is captured (or excluded) by the current filter.



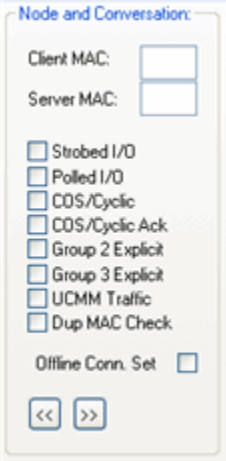
1. To create a filter, first choose which nodes to include in the filter in the Client MAC and Server MAC boxes.

Client MAC - When non-blank, messages associated with the client side of a conversation are added for this MAC ID. When blank, no client side messages are added.

Server MAC - When non-blank, messages associated with the server side of a conversation are added for this MAC ID. When blank, no server side messages are added.

Example - To filter on all server side messages from MAC ID 3, leave the Client MAC blank and put "3" in the Server Side box.

2. Choose the messages to filter on by checking the boxes. When blank, all messages associated with the specified client and server MAC IDs are added to the filter. Enabling one or more checkboxes limits the messages added to specific connection types only.



Offline Conn. Set - Enabling this checkbox adds the Group 4 Offline Connection Set messages to the filter.

3. Check the Exclude box to cause all messages except those listed in the filter panel to be captured.
4. Add the messages to the filter.



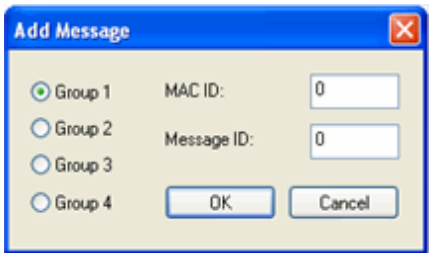
Add Conversation - Adds the messages associated with the Node and Conversation to the filter. Pressing <enter> in either of the client or server MAC fields also does this.



Remove Selection - Removes the selected message or group of messages from the filter. Pressing <delete> while navigating in the filter panel also does this.

Add Message Dialog

The Add Message dialog appears when you click the Add Message button on the toolbar of the Capture Filter tab. This dialog is used to add messages to a DeviceNet Capture Filter that are not covered by the standard connection types.



Group - Selects the Group to which the message is added.

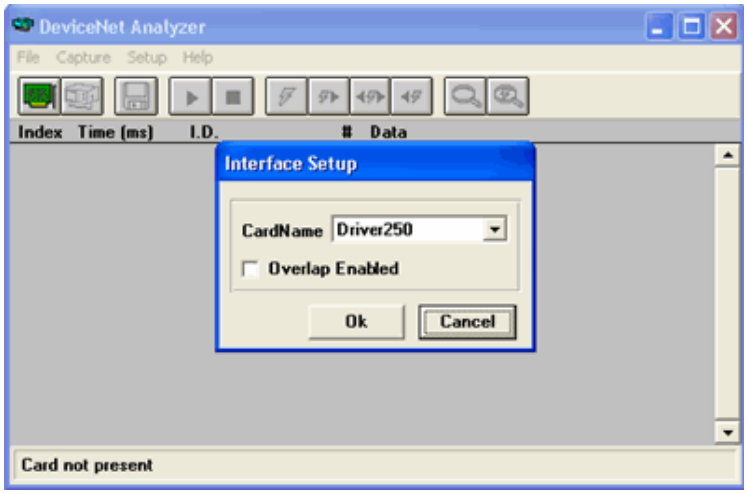
MAC ID - Selects the MAC ID for which the message is added. This field is disabled for Group 4 messages.

Message ID - Selects the Message ID to be added. The range is restricted according to the selected Group.

3.14.3 SST Woodhead DeviceNet Card Installation Instructions

The installation software on the CD is for Windows NT 4.0 with SP4, XP Pro, 2000 Pro, 2000 Server and Server 2003. We have also successfully installed the cards under XP Home Edition. If you need drivers for other operating systems, they can be downloaded from the SST Woodhead web site at http://www.woodhead.com.

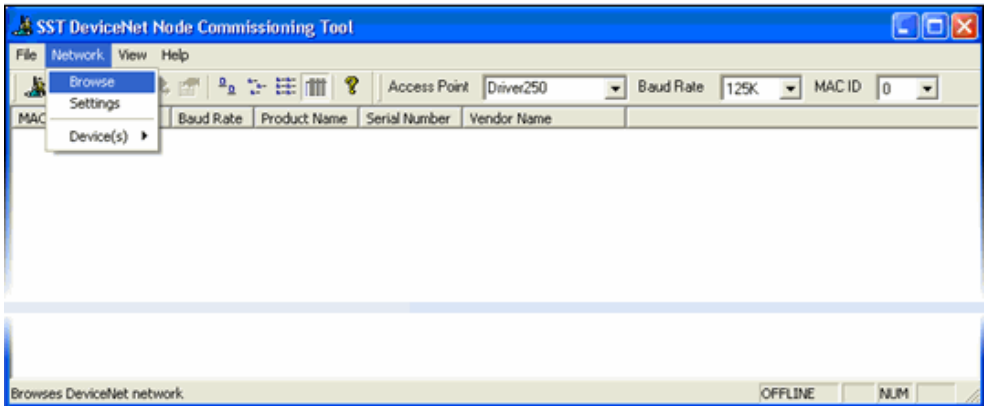
1. Insert the SST DeviceNet software CD first, before inserting the card. The CD should auto run and display the main menu. If it does not, browse the CD and double-click on setup.exe.
2. Select Product Menu from the main menu.
3. Select your card type from the Product Menu screen.
4. Choose DeviceNet DNP Products Install 2.0 for NT/XP/2000/Server from the top drop-down list and click Next. Follow the installation instructions.
5. If you do not have an operational network: Go to Start | Programs | SST | DeviceNet DNP and select the DeviceNet Analyzer program.



Select the appropriate card name from the drop list. Once selected, notice that the health LED on the dongle turns green and the comm. LED reflects the communications status of the DeviceNet Network.

If you have an operational network:

Go to Start | Programs | SST | DeviceNet DNP and select the DeviceNet Commissioning Tool. Select the appropriate module from the Access Point drop list. If the module is functioning, the software allows you to browse the network for devices. Notice that the bottom of the window displays the status of the card and network.



3.15 DeviceNet Special Instructions for RA's 1784-U2DN interface device

3.15.1 DeviceNet 1784-U2DN Hardware Settings

The Hardware Settings dialog allows you to select a device to sniff/scan. You access the Hardware Settings dialog by selecting **Hardware Settings** from the **Options** menu on the NetDecoder Control window.



FTS automatically scans and identifies all the 1784-U2DN devices plugged into the PC. These devices, identified by their Serial Numbers, are displayed in the drop-down list of Available Sniffers.

1. 1. Select a device from the drop-down list
2. 2. Select OK.

Selecting Cancel overrides all the selections and returns the user to the Control Window.

Note: You can select Refresh List to update the list of devices.

Note: For additional information about the 1784-U2DN device, please refer to the documentation from Rockwell Automation(RA). The relevant RA document numbers are:

- **Publication: 1784-IN046**
- **MM (PN): PN-25191**
- **DIR: 10000017341/PUB**
- **KnowledgeBase Tech Note: http://www.rockwellautomation.com/knowledgebase/ , ID 53280.**

NetDecoder 1784-U2DN IO Settings

NetDecoder 1784-U2DN IO Settings Start Triggers

3.15.2 DeviceNet 1784-U2DN I/O Settings

The DeviceNet1784-U2DN I/O Settings provides the user options for setting START and STOP triggers. The user can define the START and STOP triggers according to the contents of the Controller Area Network (CAN) Identifier field in the DeviceNet frame. The CAN ID of a DeviceNet frame consists of three parts: the Group Number, the MAC ID and the Message ID.

ON the I/O Settings dialog you can Add, Edit, and Delete START and STOP Triggers.

- A START trigger is defined as the event that starts data capture. The capture engine ignores all DeviceNet frames prior to the enabling of the specified START trigger. All subsequent frames are captured until either a user-defined STOP trigger fires or the user manually stops data capture.
- A STOP trigger is defined as the event that stops data capture. The capture engine stops capturing all frames after the specified STOP trigger event is enabled.

The START or STOP trigger is enabled when an incoming DeviceNet frame has a CAN ID value equal to the value in the Simple Trigger. If user has defined multiple CAN IDs, then the condition is met if the CAN ID of the incoming frame matches any one of the defined IDs. If the user enters a blank field in the trigger dialog, then that implies that the trigger condition is met on any value of CAN ID.

In the case of a START trigger, the particular frame matching the condition will be the first frame in the capture and all subsequent frames will be captured. In the case of a STOP trigger, the particular frame matching the condition will be the last frame in that capture session.

The user can define and store multiple START and STOP triggers. The triggers are displayed in the list control boxes shown on the I/O Settings Dialog. Though multiple triggers can be created and saved, only a single set of START and STOP triggers can be selected at a time.

- The I/O Settings option is not available during the middle of a data capture. Only when the data capture is stopped, the user will be able to select the I/O settings menu and bring up the triggers.
- The triggers are saved in a NetDecoder .ini file. The saved triggers appear in the I/O Settings dialog the next time the application is opened.

3.15.3 DeviceNet 1784-U2DN I/O Settings - START/STOP Triggers

There are two ways to set a START/STOP Trigger, with a Simple Trigger or a Complex Trigger.

3.15.4 Adding Simple Start/Stop Triggers

The user can add a new set of START or STOP triggers by clicking on the “Add” button to the right of the list control boxes. On clicking the “Add” button, the Set Start/Stop Trigger Conditions dialog appears. The process for creating a Start Trigger or a Stop Trigger is exactly the same.

To learn more about triggers, see NetDecoder 1784-U2DN IO Settings - Start/Stop Triggers.

3.15.5

To add a **Simple START or STOP Trigger**

1. From the I/O Settings dialog select Add.

The Set START Trigger Conditions dialog appears.

2. Select the Simple Controller Area Network CAN radio button.

From this point you can only enter a basic CAN ID. The rules for entering a basic CAN ID are:

- The CAN values are read as **hexacdecimal**.
- The values can range from **0x000 to 0x7FF**.
- You can enter a single value: **12**
- You can enter multiple values which must be separated by a semi-colon: **34;12;AB;FC;2**
- You can enter a range of values: **12-28**
- You can enter a combination of individual values and ranges: **12;34;56-7A;1**

3. Enter The CAN ID(s) in the text box.
4. Select OK.

If all the trigger values are valid, then the values are stored in the list control box on the I/O Settings Dialog. The last trigger created is shown at the bottom of the list.

Note: Selecting Cancel overrides all the selections and returns the user to the I/O Settings Dialog.

3.15.6 Adding a Complex Start/Stop Trigger

The Complex Identifier Trigger (CAN) ID Trigger radio button option provides the user with the ability to define complicated triggers based on the exact values of group numbers, MAC IDs and Message IDs.

To learn more about triggers, see NetDecoder 1784-U2DN IO Settings START/STOP Triggers.

The process for setting a START Trigger or a STOP Trigger is exactly the same.

To add a **Complex START** or **STOP Trigger**

1. From the I/O Settings dialog select Add.

The Set START Trigger Conditions dialog appears.

2. Select the CAN ID Trigger radio button.

The **CAN ID Trigger** option allows you to define complicated triggers based on the exact values of group numbers, MAC IDs and Message IDs. There are four groups to choose from. The following figure taken from the official DeviceNet specification shows how the 11 bits of the CAN ID are used by the DeviceNet messaging protocol and the values in the four groups.

IDENTIFIER BITS											HEX RANGE	IDENTITY USAGE
10	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**		
0	Group 1 Message ID				Source MAC ID						000 – 3ff	Message Group 1
1	0	MAC ID						Group 2 Message ID			400 – 5ff	Message Group 2
1	1	Group 3 Message ID			Source MAC ID						600 – 7bf	Message Group 3
1	1	1	1	1	Group 4 Message ID (0 – 2f)						7c0 – 7ef	Message Group 4
1	1	1	1	1	1	1	X	X	X	X	7f0 – 7ff	Invalid CAN Identifiers
10	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**		

3. Enter a Source/Destination (Src/Dst) MAC ID(s) in the text box.

- The Src/Dst values are entered in decimals
- The values can range from **0 - 63**
- You can enter a single value: **12**
- You can enter multiple values which must be separated by a semi-colon: **34;12;22;34;61**
- You can enter a range of values: **12-28**
- You can enter a combination of individual values and ranges: **12;34;56-59;61**

4. Select a Group radio button.

When you select a radio button for Group 1,2, 3 or 4, a set of Message ID's appear in the Select Message ID's list box. You can select one or more of the Message IDs in each group.

5. Select one or more of the Message IDs using the checkbox

6. Select OK.

Note: Selecting Cancel overrides all the selections and returns the user to the I/O Settings Dialog.

The I/O Settings dialog reappears with the Trigger Type, CAN or Msg Id(s), Group Name, and Src/Dst MAC Id(s). Not all columns will have data. For example, Group Four will not have a MAC ID. Also, if you enter a Simple START/STOP Trigger, there will be no Group identifier.

3.15.7 Editing a Simple Start/Stop Trigger

When you select a START/STOP Trigger on the I/O Settings 1784-U2DN, it appears in the START/STOP Triggers list control box. Once a trigger is created, you can select it and edit the values that were entered initially.

To edit a **Simple START/STOP Trigger**

1. From the I/O Settings dialog, double click the specific trigger in the list control box

OR

Select the trigger in the list control box and click on the "Edit" button on the right.

The *Set START/STOP Trigger Conditions* dialog appear with the triggers dialog box populated with the stored values.

You can edit the Source/Destination MAC ID's.

2. Make changes to the trigger.
3. When you are finished editing the trigger, select OK.

If all the new changes are valid, the new trigger values are stored in the same position in the list control box. If the values are not valid, you will receive and error message identifying the error.

Note: Selecting Cancel overrides all the selections and returns the user to the I/O Settings Dialog.

3.15.8 Editing a Complex Start/Stop Trigger

When you create a START/STOP Trigger on the I/O Settings 1784-U2DN, it appears in the START/STOP Triggers list. Once a trigger is created, you can select it and edit the values that were entered initially.

1. From the I/O Settings dialog, double click the specific trigger in the list control box

OR

Select the trigger in the list control box and click on the "Edit" button on the right.

The *Set START/STOP Trigger Conditions* dialog appears with the triggers dialog box populated with the stored values.

Note: To learn more about the Source/Destination MAC ID's or the Message ID's, select this link.

You can select or deselect a Message ID and/or edit the Source/Destination MAC ID's.

2. Edit the value(s) in the **Source/Destination MAC ID(s)** text box.
3. Select or de-select a message in the ID in the Select Message ID's list
4. When you are finished editing the trigger, select OK.

If all the new changes are valid, the new trigger values are stored in the same position in the list control box.

3.15.9 Deleting a Simple START/STOP Trigger

When you enter a START/STOP Trigger on the I/O Settings 1724-U2DN, it appears in the START/STOP Triggers list. Once a trigger is set, you can delete it from the list.

To delete a **Simple START or STOP Trigger**

1. From the *I/O Settings Dialog* select the checkbox for the trigger you want to delete.
2. Select Delete.

The trigger is deleted from the list.

3.15.10 Deleting a Complex Start/Stop Trigger

When you select a START/STOP Trigger on the I/O Settings 1784-U2DN, it appears in the START/STOP Triggers list. Once a trigger is set, you can delete it from the list.

To delete a **Complex START/STOP Trigger**

1. From the *I/O Settings Dialog* select the checkbox for the trigger you want to delete.
2. Select Delete.

The trigger is deleted from the list..

3.15.11 IEC 870-5-101 & 104 Special Instructions

3.15.11.1 IEC 870-5-101 & 104 Decoder Parameters

NOTE:

These instructions apply to IEC 870-5-101 and IEC 870-5-104 only. IEC 870-5-103 does not require any additional setup. For the remainder of the setup instructions, IEC 870-5-101 and IEC 870-5-104 are both referred to as simply IEC 870

Decoder Parameters

An interesting attribute of IEC 870 is that the sizes of certain fields and the mode of transmission (balanced or unbalanced) must be specified by the user. Such values are called decoder parameters. Decoder parameters are set by the user in the Decoder Parameters window. To open this window, choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window.

This window pops up automatically the first time that a capture file is loaded. The two tabs are titled "[protocol] Application Layer" and "[protocol] Link Layer" where “[protocol]” refers to the specific protocol.

IEC 870 Application Layer Parameters

"Does Originator Address exist?" specifies whether the application layer "Originator Address" field exists. Permissible values are Yes and No. The field is 1-byte long if it exists.

"Size of the ASDU address field in bytes" specifies the number of bytes in the application layer "ASDU Address" field. The permissible range is 1-2.

"Size of info object address" specifies the number of bytes in the application layer "Information Object Address" field. The permissible range is 1-3.

IEC 870 Link Layer Parameters

"Is transmission balanced?" specifies whether transmission is balanced or unbalanced.

Permissible values are Yes and No.

Balanced transmission mode is when two devices can both send at the same time.

Unbalanced transmission mode is when only one device can send at a time.

In the decode, three fields are affected by the transmission mode, and all are in the control byte of the link layer.

- Bit 8 is labeled "Direction" in balanced mode and "Reserved" in unbalanced mode.
- Bit 6 for secondary-to-primary is labeled "Reserved" in balanced mode and "Access Demand for Class 1 Data Transmission" in unbalanced mode. (For primary-to-secondary, the label is always "Frame Count Bit" regardless of transmission mode.)
- Bits 1-4 are always labeled "Function Code", but have different values for balanced mode versus unbalanced mode.

"Size of the address field in bytes" specifies the number of bytes in the link layer "Address" field. The permissible range for the protocol itself is 0-2 in balanced mode and 1-2 in unbalanced mode, but the dialog accepts a range of 0-2 regardless of mode.

3.15.11.2

3.15.11.3 What To Do When The Correct Values Of Decoder Parameters Are Unknown

It is important to note that in many cases a useful decode can be obtained even if the correct decoder parameter values are unknown to the user.

Link Layer Values

An incorrect value in the "Size of the address field in bytes" is easy to determine because fixed-length frames are invalid and shown in red. The length of fixed-length frames is in the range 4-6. They begin with byte 0x10 and end with byte 0x16 (there can also be bytes with those values elsewhere in the frame). To correct the problem, you can change the values in "Size of the address field in bytes" field until fixed-length frames no longer appear in red.

An incorrect value of "Is transmission balanced?" has no effect on the rest of the decode, and it can be left as it is if the user doesn't care about the three fields directly affected by it (see description above). There is no way to find the correct value by looking at the data, with the exception if the size of the link layer address field is 0, then the transmission mode must be balanced.

Application Layer Values

The application layer parameters are Does Originator Address Exist, Size Of ASDU Address Field In Bytes, and Size Of Info Obj Address Field In Bytes. They apply only to variable-length frames, which can be of almost any size. Variable-length frames start with byte 0x68, end with byte 0x16 (there can also be bytes with those values elsewhere in the frame), and come in two forms, identified by the value of the SQ bit, which is contained in the variable structure qualifier. The spec describes them this way:

- SQ=0: There are one or more information objects, each with a single set of information elements.
- SQ=1: There is only one information object, which contains one or more sets of information elements.

That's equivalent to saying this:

- SQ=0: There is a separate information object address for each set of information elements.
- SQ=1: There is one information object address and one or more sets of information elements.

When SQ=1, there is only one instance of the information object address, and finding a combination of values for the parameters that yields an otherwise valid decode is a generally simple matter of trial-and-error. If the detail pane indicates that there are extra data bytes (indicated by the presence of the Data field at the end), selectively increase the values of those parameters to use up the extraneous data. If the detail pane indicates that a field is missing, selectively decrease the values of those parameters until all fields are present. The fields that these parameters refer to are contiguous; therefore no intervening fields are compromised. What can make this process tricky is that some frames may in fact have the wrong number of bytes in them. When experimenting with parameter values, use frames which appear to be the same type and length as other frames in the decode since this generally indicates that those frames are of valid length.

When SQ=0, things are trickier. In this case, the information object address can appear multiple times, and not contiguously. It is technically possible to set the parameters such that there is neither extra Data nor missing fields but the decode itself is invalid. There is no surefire approach to this.

3.16 Modbus Special Instructions

3.16.1 Modbus Register Display Format Settings

Modbus protocol messages do not provide data formatting information but simply transmit holding and input registers as byte streams. The Modbus Register Display Settings dialog provides a method for users to define display formats to be utilized when displaying the values in these registers.

To access this dialog:

1. Go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters*
2. Select the *Modbus* tab.
3. To add a new entry, fill in the fields and click the *Add* button. Double-clicking a setting, copies its values to the input fields.
4. To replace a setting with a new setting created from the input fields, click the setting to replace and then click the *Modify* button.

When you close a capture file, you are asked whether you want to save the current register settings into it. To save settings independent of a specific capture file:

1. Type any string in the "Apply Template" field and click *Save*.

2. To restore those settings to the dialog, select the desired setting in the "Apply Template" drop down list.

New settings do not take effect in a currently opened capture file until the frame display is closed and then reopened.

Register Display Settings

- **Default Display Format_Bits**

  This field specifies the default display format for registers that have no user defined setting (such registers are always assumed to be 2 bytes long). The default display format is limited to single-register display formats to prevent implicit register range overlap and to ensure that explicitly defining a setting in which one display format item uses multiple registers does not change the locations of subsequent default settings.

- **Station Address**

  The IP Address or Station Address field (its name changes to reflect the loaded decoder) is used to enter the desired IP or station address for each setting. Enter an asterisk to specify that a setting applies to all IP or station addresses. Station address ranges are from 0 to 248 and IP address ranges can be any valid IP Address.

- **Register Type**

  The Register Type field specifies the type of register, either HOLDING or INPUT.

- **Bytes Per Register**

  This field defaults to 2, indicating that standard Modicon registers are 2 bytes each. If you are dealing with a third party implementation of Modbus, you may need to adjust this field to reflect the actual number of bytes in a single register.

- **Register Start Address**

  Enter the address of the first register you want to specify settings for.

- **Display Format_Bits**

  The Display Format_Bits field specifies the desired display format. Display formats ASCII and HEX are variable-length and display a char or hex byte respectively for each byte in a register. The other display formats (INT_16, FLOAT_32, etc) have a bit count suffix in their names and use as many registers as they need, based on the bytes per register field. Choose a format for the specified register range.

- **Length**

  This field is the desired number of data items (e.g. INT_32s), not the number of registers. The number of registers are calculated and displayed in the text description.

Example

If you want to specify Station 3's input registers 0-99 as INT_16s, you would enter 3 for the Station Address, INPUT for the Register Type, 0 for the Start Address, 2 for Bytes Per Register, INT_16 for the Display Format and 100 for the Length, indicating that you have 100 INT_16s starting at Input Register Address 0 where each register is 2 bytes long.

3.16.2 Setup For Modbus RTU and ASCII

Modbus ASCII and Modbus RTU protocols have three selections on the launcher menu. The appropriate selection depends upon physical characteristics of your network.

If your system is running over a physical layer that is 2 wire RS-422/485, select either the Modbus RTU on 2Wire RS422/485 or the Modbus ASCII on 2Wire RS422/485, depending upon which protocol your system is using. In this case there are no special wire tapping instructions. If your system is not a 2 wire RS422/485 system, you must select the correct launcher item based upon the following information.

There are two decodes for Modbus RTU: Modbus RTU Master and Modbus RTU Slave. Similarly, there are two decodes for Modbus ASCII: Modbus ASCII Master and Modbus ASCII Slave. The Master and Slave refer to where in the circuit the analyzer is connected. The rest of this topic simply refers to Modbus Master or Modbus Slave, as the principles are the same.

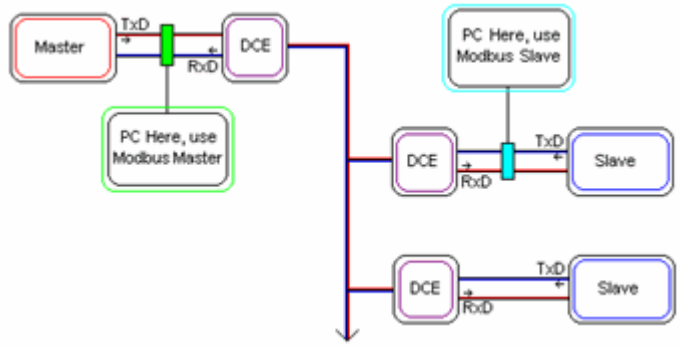
Modbus Master assumes that data from the Master is on the DTE side (i.e. master data is on the TxD pin and slave data on the RxD pin). If the analyzer is connected to a Master device, choose the Modbus Master decode.

Modbus Slave assumes that data from the slave is on the DTE side (i.e. slave data is on the TxD pin and master data on the RxD pin). If the analyzer is connected to any Slave device, choose the Modbus Slave decode.

The diagram below illustrates conceptually which decoder to choose. Your configuration may be different from the diagram. The important thing is to choose Modbus Master if the master data is on the transmit line, or Modbus Slave if the slave data is on the transmit line.

Once you have selected the correct protocol, be sure to set the Register Display Settings so your data is decoded correctly.

If you have a custom protocol and need help connecting the analyzer to the right location, see Generic Channel Dependent Decodes Setup.



3.16.3 Setup for Modbus TCP

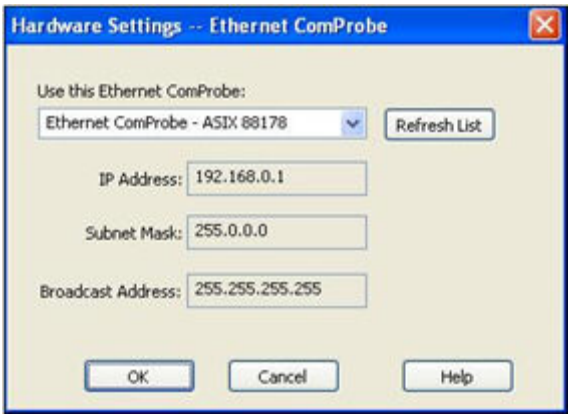
In order to correctly decode Modbus TCP, the software needs to know the IP Addresses of the Master and Slave devices. The system allows the user to define any number of IP Address and Node Type combinations and save them in a template for later use.

The Template function provides the capacity to create multiple templates that contain different node assignments. This capability allows the user to maintain individual templates for each network monitored. Applying a template containing the node assignments necessary to monitor transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

3.17 Ethernet ComProbe Special Instructions

3.17.1 Ethernet ComProbe Hardware Settings

The Hardware Settings dialog allows you to select a specific Ethernet ComProbe device to sniff your Ethernet traffic.



1. You access the Hardware Settings dialog by selecting Hardware Settings from the Options menu on the NetDecoder Control window.
2. Select a **device** from the drop-down list

Note: FTS automatically scans and identifies all the Ethernet ComProbe devices plugged into the PC.

The IP address, subnet Mask and the Broadcast Address for that particular device are displayed.These are display only and cannot be edited.

3. If that is the right device you wish to use, select **OK**. Selecting Cancel overrides all the selections and returns the user to the Control Window.

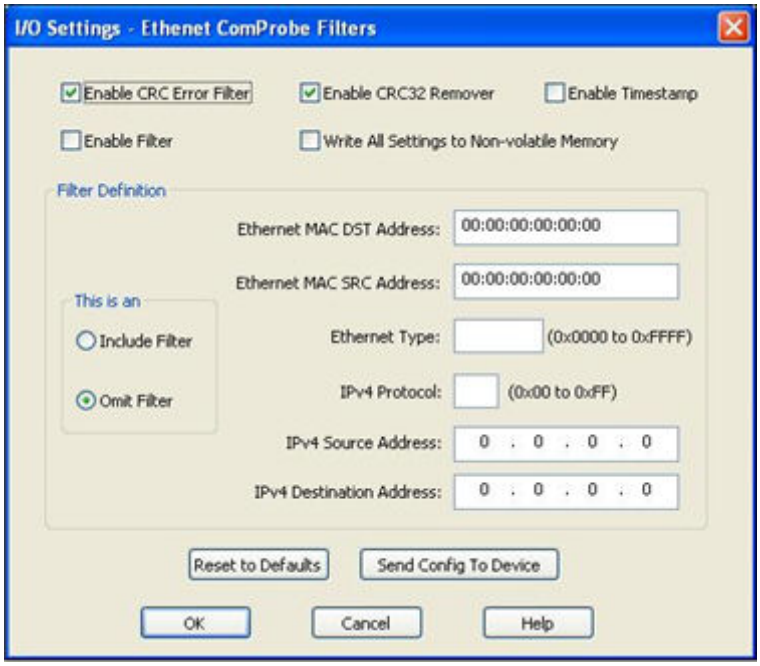
There are a couple of things to remember about this dialog.

- You can select **Refresh List** at any time to update the list of devices.
- When you run NetDecoder with the **Ethernet ComProbe** option, the software disables the ability to sniff with other Ethernet NIC cards. If you wish to capture Ethernet traffic over other NIC cards, you must select the regular **Ethernet** option in the NetDecoder start up wizard.

3.17.2 Ethernet ComProbe I/O Settings

The I/O Settings dialog allows you to configure the Ethernet ComProbe with filters and special timestamping ability.

1. You access the I/O Settings dialog by selecting I/O Settings from the Options menu on the NetDecoder Control window.



There are a number of settings you can select on this dialog that will affect how the frames are captured and displayed.

At the top of the dialog are five check boxes:

- **Enable CRC Error Filter:** When enabled, the CRC error filter discards all Ethernet frames that have CRC errors. These error frames will not be captured.

- **Enable CRC32 Remover:** When the CRC32 Remover is enabled, the Ethernet ComProbe removes the 4-bytes of CRC data from every Ethernet frame before passing it up to the software.
- **Enable Timestamp:** When enabled, the Ethernet ComProbe adds a five (5) NanoSecond timing to each capture packet. This also adds eight (8) extra bytes at the end of each Ethernet frame.
- **Enable Filter:** Selecting this check box either enables or disables the capture filters.
- **Write all settings to Permanent Memory:** If this option is selected, the configuration is written to the permanent non-volatile memory in the device.

This is an:

- **Include Filter**: When you select this radio button, the Ethernet packets that match the filter settings are captured and displayed.
- **Omit Filter**: When you select this radio button, the Ethernet packets that match the filter settings are discarded. Only packets that do not match the settings are captured and displayed.

On the right side are **six text entry boxes**:

- **Ethernet MAC DST Address:** Enter the Ethernet MAC Destination Address
- **Ethernet MAC SRC Address:** Enter the Ethernet MAC Source Address
- **Ethernet Type:** Enter the 2-byte Ethernet Type value in hex. The value can range from 0x0000 to 0xFFFF.
- **IPv4 Protocol:** Enter the one byte IPv4 protocol type. The value can range from 0x00 to 0xFF.

For a complete listing of the Ethernet Types and the IPv4 Protocol types, visit The Internet Assigned Numbers Authority (IANA) website (www.iana.org).

- **IPv4 Source Address:** Enter the Source IP Address
- **IPv4 Destination Address:** Enter the Destination IP Address

After selecting/entering values, it's very important that you understand what the buttons at the bottom of the dialog do when you select them.

- **Reset to Defaults**: When you select *Reset to Defaults*, Enable CRC Error Filter and Enable CRC32 Remover check boxes at the top of the dialog are enabled. All other options are disabled.

- **Send Config to Device**: After setting all the options in the dialog, you **must click on Send Config to Device before OK** to transfer the settings to the Ethernet ComProbe.

- **OK**: There are two things to consider with the **OK** button.

    - If you click OK **before** you select **Send Config to Device**, the dialog will close and the settings will be saved, but they **will not be transferred** to the ComProbe. The settings will, however, be there if you open the dialog again.

    - If you select OK **after** you select **Send Config to Device**, the dialog will close, the **settings will be saved and transferred to the ComProbe**.

- Selecting **Cancel** overrides all the selections and returns the user to the Control Window.

4 Protocol Stacks

4.1 Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.

To start the wizard:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon  on the Frame Display.
2. Select a protocol stack from the list, and click Finish. Click for information on how the analyzer auto-traverses the protocol stack.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating a Custom Stack.

1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the *Remove Selected Item From List* button becomes active.
2. Click the Remove button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing for more information.

You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

Note for BCSP:

If you are using the BCSP protocol stack, you must connect the analyzer to the circuit such that the data on the DTE line comes from the host, and data on the DCE line comes from the controller. Click here

Note for Modbus RTU:

If you are using the Modbus RTU protocol stack, you must select either Modbus RTU Master or Modbus RTU Slave depending on where the analyzer taps into the circuit. Click here for more information.

Note for Modbus TCP:

If you are using Modbus TCP over Ethernet, you need to set up a node database giving the IP addresses for the Master and Slave devices. Click here for more information.

Note for Data Highway Plus (DH+):

There are special hardware and software configuration instructions for setting up the DL3000 DHM device used to tap into the Data Highway Plus network. Click here for more information.

Note for IEC 870-5-101:

You need to give the decoder information on the sizes of some fields and whether or not other fields are present. There are all system configurable options and therefore the decoder has no way of knowing this information from the data. Click here for more information.

Note for DeviceNet

You need to install the DeviceNet card before beginning data capture. Then you need to setup the device in the Hardware Settings window, and optionally select any capture filters.

4.2 Information Screen

The second screen of the Protocol Stack Wizard gives information to help you decide if you need to define a custom stack or if a pre-defined stack has what you need.

4.3 How the Analyzer Auto-traverses the Protocol Stack

In the course of doing service discovery, devices ask for and receive a Protocol Descriptor List defining which protocol stacks the device supports. It also includes information on which PSM to use in L2CAP, or the channel number for RFCOMM, or the port number for TCP or UDP. The description below talks about how the analyzer auto-traverses from L2CAP using a dynamically assigned PSM, but the principle is the same for RFCOMM channel numbers and TCP/UDP port numbers.

The analyzer looks for SDP Service Attribute Responses or Service Search Attribute Responses carrying protocol descriptor lists. If the analyzer sees L2CAP listed with a PSM, it stores the PSM and the UUID for the next protocol in the list.

After the SDP session is over, the analyzer looks at the PSM in the L2CAP Connect frames that follow. If the PSM matches one the analyzer has stored, the analyzer stores the source channel ID and destination channel ID, and associates those channel IDs with the PSM and UUID for the next protocol. Thereafter, when the analyzer sees L2CAP frames using those channel IDs, it can look them up in its table and know what the next protocol is.

In order for the analyzer to be able to auto-traverse using a dynamically assigned PSM, it has to have seen the SDP session giving the Protocol Descriptor Lists, and the subsequent L2CAP connection using the PSM and identifying the source and channel IDs. If the analyzer misses any of this process, it is not able to auto-traverse. It stops decoding at the L2CAP layer.

For L2CAP frames carrying a known PSM (0x0001 for SDP, for example, or 0x0003 for RFCOMM), the analyzer looks for Connect frames and stores the PSM along with the associated source and destination channel IDs. In this case the analyzer does not need to see the SDP process, but does need to see the L2CAP connection process, giving the source and destination channel IDs.

4.4 Creating and Removing a Custom Stack

To create a custom stack:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon  on the Frame Display.
2. Select *Build Your Own* from the list and click *Next*.
3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click *Next* to continue.

Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the Protocol Decode Stack box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the *Move Up* and *Move Down* buttons until the protocol is in the correct position.
5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

Auto-traversal (Have the analyzer Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers:

1. Click the All additional stack layers can be determined automatically button.
2. If your protocol stack is complete and there are no additional layers, click the There are no additional stack layers button.
3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

To save your stack:

1. Click the Add To Predefined List button.
2. Give the stack a name, and click Add.

In the future, the stack appears in the Protocol Stack List on the first screen of the Protocol Stack wizard.

Remove a Stack

To remove the stack:

1. Select it in the first screen and click *Remove Selected Item From List*.
2. If you remove the stack, you must to recreate it if you need to use it again.

Note:

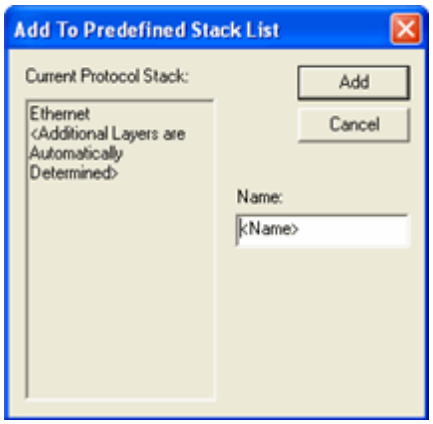
If you do not save your custom stack, it does appear in the predefined list, but applies to the frames in the current session. However, it is discarded at the end of the session.

4.5 Saving User Defined Stacks

You can create protocol stacks for one time use that disappear at the end of the session. If you want to use the stack again in a subsequent session, then you need to recreate it. However, if you save the stack, then it is available every time you start the analyzer, until you delete it.

The *Add To Predefined Stack List* dialog allows the user to save a custom stack for future use.

1. After creating a custom stack using the Protocol Stack Wizard, click the *Add To Predefined List* button on the last screen of the wizard.



Your newly defined stack appears in the *Current Protocol Stack* pane on the left.

2. Simply enter a name for the stack and click *Add*.

The name of the stack now appears as a selection in the *Select a Protocol Stack* dialog.

4.6 Reframing

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. You can also use Reframe to frame unframed data. The original capture file is not altered during this process.

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To reframe your data, load your capture file, select a protocol stack, and then select Reframe from the File menu on the Control window. Reframe is only available if the frame recognizer used to capture the data is different from the current frame recognizer.

In addition to choosing to Reframe, you can also be prompted to Reframe by the Protocol Stack Wizard.

1. Load your capture file by choosing Open from the File menu on the Control window, and select the file to load.
2. Select the protocol stack by choosing Protocol Stack from the Options menu on the Control window, select the desired stack and click Finish.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the Protocol Stack Wizard asks you if you want to reframe your data. Choose Yes.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing for instructions on removing framing from data.

4.7 Unframing

This function removes start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process.

You cannot unframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To manually unframe your data, select Unframe from the File menu on the Control window. Unframe is only available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

In addition to choosing to Unframe, you can also be prompted to Unframe by the Protocol Stack Wizard.

1. Load your capture file. To do this, choose Open from the File menu on the Control window, and select the file to load.

2. Remove the protocol stack. To do this, choose Protocol Stack from the Options menu on the Control window, select None from the list, and click Finish.
3. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file. Choose Yes.
4. The system removes the frame markers from your data, puts the unframed data into a new file, and opens the new file. The original capture file is not altered.

See Reframing for instructions on framing unframed data.

4.8 Providing Context For Decoding When Frame Information Is Missing

There may be times when you need to provide information to the analyzer because the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame indicating the command.

The analyzer provides a way for you to supply the context for any frame, provided the decoder supports it. (The decoder writer has to include support for this feature in the decoder, so not all decoders support it. Note that not all decoders require this feature.)

If the decoder supports user-provided context, three items are active on the Options menu of the Control Window, Frame Display and Protocol Navigator windows. These items are *Set Initial Decoder Parameters*, *Automatically Request Missing Decoding Information*, and *Set Subsequent Decoder Parameters*. (These items are not present if no decoder is loaded that supports this feature.)

Set Initial Decoder Parameters is used to provide required information to decoders that is not context dependent but instead tends to be system options for the protocol.

Choose Set Initial Decoder Parameters in order to provide initial context to the analyzer for a decoder. A dialog appears that shows the data for which you can provide information.

If you need to change this information for a particular frame :

1. Right-click on the frame in the Frame Display window
2. Choose Provide <context name>.

Alternatively, you can choose Set Subsequent Decoder Parameter from the Options menu.

3. This brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check *Automatically Request Missing Decoding Information*.
5. When unchecked, the analyzer doesn't bother you with dialogs asking for frame information that you don't have. In this situation, the analyzer decodes each frame until it cannot go further and then simply stop decoding.

5 Capturing Data

5.1 Capturing Data

Note: Data Capture is not available in Viewer mode.

1. Click the Start Capture icon  to begin capturing to a file. This icon is located on the Control  , Event Display  , and Frame Display  windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the Options menu on the Control window to change the default file location.
3. Watch the status bar on the Control window to monitor how full the file is. When the file is full, it begins to *wrap*, which means the oldest data will be overwritten by new data.
4. Click the Stop icon  to temporarily stop data capture. Click the Start Capture icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.
5. To clear captured data, click the Clear icon  .
    - If you select Clear after selecting Stop, a dialog appears asking whether you want to save the data.
        - You can click Save File and enter a file name when prompted .
        - If you choose Do Not Save, all data will be cleared.
        - If you choose Cancel, the dialog closes with no changes.
    - If you select the Clear icon while a capture is occurring:
        - The capture stops.
        - A dialog appears asking if you want to save the capture
        - You can select Yes and save the capture or select No and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
        - If you choose Cancel, the dialog closes with no changes.

To change the size of the capture file, choose System Settings from the Options menu on the Control window.

5.2 USB HCI Internal Software Tap Data Source Dialog

The USB HCI Internal Software Tap Data Source Dialog allows the user to select which *Bluetooth*® device to sniff and to initiate and terminate the sniffing process.

This dialog has a list control containing the *Bluetooth* Devices connected to your system. If the *Show Connected Only* checkbox is unchecked then all USB devices that have ever been connected to your system are listed.

1. Select the device you wish to sniff.
2. Click on the Start Sniffing button. You must click on the *Start Capture*  icon on the Control window to capture data. For more details see USB HCI Sniffing.
3. Click the *Refresh List* button if you have connected or disconnected a device while this dialog is open to update the list.

6 Analyzing Byte Level Data

6.1 Event Display

To open this window

Click the Event Display icon  on the Control window toolbar.

The Event Display window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and the analyzer information, such as when the Data Capture Was Paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

Click on an event to find out more about it. The three status lines at the bottom of the window are updated with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in Hex, Decimal, Octal, and Binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, the analyzer continually updates the Event Display as data is captured. Make sure the Lock icon  is displayed on the toolbar to prevent the display from updating (Clicking on the icon again will unlock the display). While locked, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the Lock icon again.

You can have more than one Event Display open at a time. Click the Duplicate View icon  to create a second, independent Event Display window. You can lock one copy of the Event Display and analyze your data, while the second Event Display updates as new data is captured.

6.2 The Event Display Toolbar

 Home – Brings the Control window to the front.

 Open File - Opens a capture file.

 Start Capture - Begins data capture to disk.

 Stop Capture - Closes a capture file and stops data capture to disk.



Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.



Clear- Discards the temporary file and clears the display.



Lock - In the Lock state, the window is locked so you can review a portion of data. Data capture continues in the background. Clicking on the Lock icon unlocks the window.



Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon locks the window.



Duplicate View - Creates a second Event Display window identical to the first.



Frame Display - (framed data only) Brings up a Frame Display, with the frame of the currently selected bytes highlighted.



Focus Protocol Navigator - (framed data only) Brings up the Protocol Navigator window, with the currently selected frame highlighted.



Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.



Add/Modify Bookmark - Add a new or modify an existing bookmark.



Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.



Find - Search for errors, string patterns, special events and more.



Go To - Opens the Go To dialog, where you can specify which event number to go to.



CRC - Change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC appears in the status lines at the bottom of the Event Display.



Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.



Character Only - The analyzer shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.



Number Only - Controls whether the analyzer displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.

All Events - Controls whether the analyzer shows all events in the window, or only data bytes. Events include control signal changes and framing information.



Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

6.3 Opening Multiple Event Display Windows

Click the Duplicate View icon  from the Event Display toolbar to open a second Event Display window.

You can open as many Event Display windows as you like. Each Event Display is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The Event Display windows are numbered in the title bar. If you have multiple Event Displays open, click on the Event Display icon  on the Control window toolbar to show a list of all the Event Displays currently open. Select a window from the list to bring it to the front.

6.4 Calculating CRCs or FCSs

The cyclic redundancy check (CRC) is a function on the Event Display window used to produce a checksum. The frame check sequence (FCS) are the extra checksum characters added to a frame to detect errors.

1. Open the Event Display  window.
2. Click and drag to select the data you want to generate a CRC for.
3. Click on the CRC icon  .
4. In the CRC dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose an algorithm to use. Choose CRC 32 (Ethernet). Choose CRC 32 (Ethernet) for Ethernet data or the appropriate CRC type for serial data.
5. Enter a seed value in hexadecimal if desired.
6. Click OK to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC using the algorithm you selected is calculated automatically.

"CRC!" in Ethernet data

Ethernet network cards do not normally send the CRC with the frame to the upper layers of the system. The hardware on the card checks that the CRC is correct and then throws it away. FTS marks the place where the CRC would be in the data with "CRC!". When viewing Ethernet capture files made with other programs, the CRC may or may not be included, depending on the specifications of the capturing software/hardware.

Reversed CRCs on the Event Display with Ethernet data

The CRC calculated in the Event Display window is reversed from the CRC shown in the data. CRCs are calculated in network data order from Most Significant Byte (MSB) to Least Significant Byte (LSB). The Ethernet specification says to send data in host data order (LSB to MSB). Therefore the CRC as captured in the data is the reverse of the CRC as calculated.

Example: If the CRC in the data is shown as 00 01 02 03, the Event Display calculated the CRC and show it in the status lines as 03 02 01 00. This is correct.

Calculating CRC for interwoven data

FTS calculates the CRC for either side of the interwoven data. Which side it calculates is determined by the first byte selected. If the first byte is from one side, then FTS calculates the CRC for just the bytes on that side. If the first byte is from the other side, then FTS calculates the CRC for just the bytes on that side.

Incorrect results with CRC16 for serial data

If you are calculating CRCs using the CRC16 algorithm and the CRCs do not match what you know they should be, try CRC16rev. What hardware often calls CRC16 is what software calls CRC16rev.

6.5 Calculating Delta Times and Data Rates

1. Click on the Event Display icon  on the Control window to open the Event Display window.
2. Use the mouse to select the data you want to calculate a delta time and rate for.
3. The Event Display window displays the delta time and the data rate in the status lines at the bottom of the window.

6.6 Switching Between Live Update and Review Mode

The Event Display and Frame Display windows can update to display new data during live capture, or be frozen to allow data analysis. By default, the Event Display continually updates with new data, and the Frame Display is locked.

1. Make sure the Lock icon  is active so the display is locked and unable to scroll.
2. Click the Unlock  icon again to resume live update.

The analyzer continues to capture data in the background while the display is locked. Upon resuming live update, the display updates with the latest data.

You can have more than one Event Display or Frame Display window open at a time. Click the Duplicate View icon  to open additional Event or Frame Display windows. The Lock/Resume function is independent on each window. This means that you can have two Event Display windows open simultaneously, and one window can be locked while the other continues to update.

6.7 Data Formats and Symbols

6.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all *events*.

This includes:

- Data bytes
- Start-of-frame
- End-of-frame characters
- Data Captured Was Paused.

Click on the Display All Events icon to remove the non-data events. Click again to display all events.

See List of All Event Symbols for a list of all the special events shown in the analyzer and what they mean.

6.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the *radix* used to display data.

1. Go to the View menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.
2. Right-click on the "Hex" header label and choose a different radix.

If you want to see only the numerical values, click on the Numbers Only icon  on the Event Display toolbar.

6.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the Event Display window, the analyzer displays data in ASCII by default. There are several ways to change the character set used to display data.

1. Go to the View menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. Right-click on the "ASCII" header label and choose a different character set.

If you want to see only characters, click on the Characters Only icon  on the Event Display toolbar.

6.7.4 Viewing Only ASCII (or EBCDIC or Baudot)

On the Event Display toolbar you can choose to view data in ASCII, EBCDIC, or Baudot format only.

1. Click on the Characters Only icon  on the Event Display toolbar.

To add the numerical values back to the display:

1. Click the Characters Only icon again.

6.7.5 Viewing Only Hex (Or Decimal or Octal or Binary)

On the Event Display toolbar you can choose to view data as numeric only.

1. Click on the Numbers Only icon  on the Event Display toolbar.

To display the characters back to the display:

1. Click the Number Only icon again.

6.7.6 Selecting Mixed Channel/Sides

If you want to get more data on the Event Display window, you can switch to mixed sides mode. This mode puts all the data together on the same line. Data from one side is shown on a white background and data from the other is shown on a gray background.

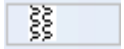
1. Click once on the Mixed Sides icon  to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click on the labels in the center of the data display window to change between mixed and side over side modes.
4. Choose Display Sides Together to go to Mixed Sides Mode or Display Sides Separately to go to side over side mode.

6.7.7 List of All Event Symbols

By default, the Event Display shows all *events*, which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button  . Click again to display all events.

Click on a symbol, and the analyzer displays the symbol name and sometimes additional information in the status lines at the bottom of the Event Display window. For example, clicking on a control signal change symbol displays which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

	Abort
	Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.

6.7.8 Font Size

The font size can be changed on several windows. Changing the font size on one window does not affect the font size on any other window.

To change the font size:

1. Click on *Options,* and select Change the Font Size.
2. Choose a font size from the list.
3. Click OK.

7 Analyzing Protocol Decodes

7.1 Frame Display Window

7.1.1 Frame Display Window

To open this window

Click the Frame Display icon  on the Control window toolbar, or select Frame Display from the Window menu.

Frame Display Panes

The Frame Display window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame. The image below gives the name of each pane. Click on the links below the image to learn more about each pane.

- Summary Pane

  The Summary Pane displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.

- Decode Pane

  The Detail Pane displays a detailed decode of the highlighted frame. Fields selected in the Decode pane have the appropriate bit(s) or byte(s) selected in the Radix, Binary, Character and Event panes.

- Radix Pane

  The Radix Pane displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.

- Binary Pane

  The Binary Pane displays a binary representation of the logical data bytes.

- Character Pane

  The Character Pane displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.

- Event Pane

  The Event Pane displays the physical data bytes in the frame, as received on the network.

By default, all panes except the Event pane are displayed when the Frame Display is first opened.

Protocol Tabs

The Frame Display adds a tab to the top of the Summary Pane for every protocol found in the in the data. You can click on these tabs to filter on the protocol. Select the Unfiltered tab to display all protocols. The Unfiltered tab is automatically selected when multiple protocols are being *filtered-in* using other filtering methods.

Comparing Frames

If you need to compare frames, you can open additional Frame Display windows by clicking on the Duplicate View icon  . You can have as many Frame Display windows open at a time as you wish.

7.1.2 Frame Display Toolbar

The buttons that appear in the Frame Display window vary according to the particular configuration of the analyzer.

 Home – Brings the Control window to the front.

 Open File - Opens a capture file.

 I/O Settings - Opens the I/O Settings dialog.

 Start Capture - Begins data capture to a user designated file.

 Stop Capture - Closes a capture file and stops data capture to disk.

 Save - Save the currently selected bytes or the entire buffer to file.

 Clear- Discards the temporary file and clears the display.

 Event Display – Brings the Event Display window to the front.

 Protocol Navigator – Brings the Protocol Navigator window to the front.

 Statistics - Brings the Statistics window to the front. This icon does not display in this location when running the analyzer in Air Sniffer. See Packet Error Rate Statistics below.

 Signal Display - Opens the Signal Display. This icon does not display when running the analyzer in Air Sniffer.


Breakout Box - Opens the Breakout Box dialog.


Duplicate View - Creates a second Frame Display window identical to the first.


Apply/Modify Display Filters - Opens the Display Filter dialog.


Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.


Find - Search for errors, string patterns, special events and more.


Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.


Add/Modify Bookmark - Add a new or modify an existing bookmark.


Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.


Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data


Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.


Packet Timeline – Opens the Packet Timeline display.


Extract Data - Opens the Extract Data dialog.


Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.


Audio Extraction - Opens the Audio Extraction dialog.


Pie Chart - This icon displays a chart that displays the number of frames with and without errors.


Network View - Opens the Network View Window.


Dashboard - Opens the Dashboard Dialog

Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.

The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.


Show Default Panes - Returns the panes to their default settings.


Show Only Summary Pane - Displays only the Summary pane.


Toggle Expanded Decode Pane - Makes the Decode pane taller and the Summary pane narrower.


Toggle Display Freeze - Prevents the display from updating.


Go To Frame - Opens the Go To dialog, where you can specify which event number to go to.


First Frame - Moves to the first frame in the buffer.


Previous Frame - Moves to the previous frame in the buffer.


Next Frame - Moves to the next frame in the buffer.


Last Frame - Moves to the last frame in the buffer.

Note that if the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

Summary drop-down box

Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a FBLEA predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled.

Text with Protocol Stack

To the right of the Summary Layer box is some text giving the protocol stack currently in use.

7.1.3 Frame Display Status Bar

The Frame Display Status bar appears at the bottom of the Frame Display. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses

7.1.4 Hiding and Revealing Protocol Layers in the Frame Display

Hiding protocol layers refers to the ability to prevent a layer from being displayed on the Decode pane. Hidden layers remain hidden for every frame where the layer is present, and can be revealed again at any time. You can hide as many layers as you wish.

Note: Hiding from the Frame Display affects only the data shown in the Frame Display and not any information in any other window.

There are two ways to hide a layer.

1. Right-click on the layer in the Decode pane, and choose Hide [protocol name] Layer In All Frames.
2. Click the Set Protocol Filtering button on the Summary pane toolbar. In the Protocols to Hide box on the right, check the protocol layer(s) you want hidden. Click OK when finished.

To reveal a hidden protocol layer:

1. Right-click anywhere in the Decode pane
2. Choose Show [protocol name] Layer from the right-click menu, or click the Set Protocol Filtering button and un-check the layer or layers you want revealed.

7.1.5 Physical vs. Logical Byte Display

The Event Display window and Event Pane in the Frame Display window show the *physical bytes*. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the *logical data*, or the resulting byte values after escape codes or other character altering codes have been applied (a process called *frame transformation*).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane displays 0x7d 0x23, while the Radix pane displays 0x03.

7.1.6 Sorting Frames

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the Summary pane to sort the frames by that column. For example, to sort the frames by size, click on the *Frame Size* column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

7.1.7 Synchronizing the Event and Frame Displays

The Frame Display is synchronized with the Event Display. Click on a frame in the Frame Display and the corresponding bytes is highlighted in the Event Display. Each Frame Display has its own Event Display.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the Frame Display icon  in Control window toolbar to open the Frame Display.
2. Click on the Duplicate View icon  to create Frame Display #2.
3. Click on Event Display icon  in Frame Display #2. Event Display #2 opens. This Event Display is labeled #2, even though there is no original Event Display, to indicate that it is synchronized with Frame Display #2.
4. Click on a frame in Frame Display #2. The corresponding bytes are highlighted in Event Display #2.
5. Click on a frame in the original Frame Display. Event Display #2 does not change.

7.1.8 Working With Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the *Duplicate View* icon  on the Frame Display toolbar.

This creates another Frame Display window. You can have as many Frame Displays open as you wish. Each Frame Display is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the *Frame Display* icon  in the Control window toolbar.

A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one Frame Display, that filter does not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

7.1.9 Working With Panes

When the Frame Display first opens, all panes are displayed except the Event pane. The panes include:

- To view all the panes, select *Show All Panes* from the *View* menu.
- The *Toggle Expand Decode Pane* icon  makes the decode pane longer to view lengthy decodes better.
- The *Show Default Panes* icon  returns the Frame Display to its default settings.
- The *Show only Summary Pane* icon  displays on the Summary Pane.

1. To close a pane, right-click on the pane and select *Hide This Pane* from the pop-up menu, or de-select *Show [Pane Name]* from the *View* menu.
2. To open a pane, right-click on the any pane and highlight *Show Hidden Panes* from the pop-up menu and select the pane from the fly-out menu, or select *Show [Pane Name]* from the *View* menu.
3. To resize a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to resize the pane.

7.1.10 The Panes in the Frame Display

7.1.10.1 Summary Pane

The Summary pane  displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

The Summary pane in FTS4USB displays a one-line summary of every transaction in a capture buffer or file. Whenever there is a transaction it is shown on a single line instead of showing the separate messages that comprise the transaction. The Msg column in that case says "Transaction".

Each message in a transaction contains a packet identifier (PID). All of the PIDs in a transaction are shown in the transaction line.

All IN transactions (i.e. transactions that contain an IN token message) are shown with a purple background. All other transactions and all non-transactions are shown with a white background. IN transactions have special coloring because that is the only place where the primary data flow is from a device to the Host.

The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred is displayed in red. The Decode Pane gives precise information as to the type of error and where it occurred.

The Summary pane is synchronized with the other panes in this window. Click on a frame in the Summary pane, and the bytes for that frame is highlighted in the Event pane while the Decode pane displays the full decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

Use the navigation icons, keyboard or mouse to move through the frames. The icons  and  move you to the first and last frames in the buffer, respectively. Use the Go To icon  to move to a specific frame number.

7.1.10.2 Customizing Fields in the Summary Pane

You can modify the Summary Pane in Frame Display.

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The Frame Size, Timestamp, and Delta columns can be hidden by right-clicking on the header and selecting *Show Frame Size Column, Show Timestamp Column,* or *Show Delta Column*. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose *Restore Default Column Widths*, or select *Restore Default Column Widths* from the *Format* menu.

7.1.10.3 Frame Symbols in the Summary Pane



A green dot means the frame was decoded successfully, and the protocol listed in the Summary Layer drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the Summary Layer drop-down box does not exist in the frame.



A green circle means the frame was not fully decoded. There are several reasons why this might happen.

One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot.

Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has

changed. If the analyzer does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.

A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

7.1.10.4 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

7.1.10.5 Decode Pane

The Decode pane (aka detail pane)  is a post-process display that provides a detailed decode of each frame transaction (sometimes referred to as a frame). The decode is presented in a layered format that can be expanded and collapsed depending on which layer or layers you are most interested in. Click on the plus sign to expand a layer. The plus sign changes to a minus sign. Click on the minus sign to collapse a layer. Select Show All or Show Layers from the Format menu to expand or collapse all the layers. Layers retain their expanded or collapsed state between frames.

Protocol layers can be hidden, preventing them from being displayed on the Decode pane. Right-click on any protocol layer and choose Hide [protocol name] from the right-click menu.

In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is applied to layers when the detail pane displays a single message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction between layers and messages clear, each header of each message in the detail pane ends with the word “Message” or “Messages”. The latter is used because data and handshake messages are shown as a single color-coded entry

Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character Panes. The colors are not assigned to a protocol, but are assigned to the layer.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

Click the Toggle Expand Decode Pane icon  to make the Decode pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

7.1.10.6 Radix or Hexadecimal Pane

The Radix pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the Format menu, or by right-clicking on the pane and choosing Hexadecimal, Decimal or Octal.

Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.10.7

7.1.10.8 Character Pane

The Character pane represents the logical bytes in the frame in ASCII, EBCDIC or Baudot. The character set can be changed from the Format menu, or by right-clicking on the pane and choosing the appropriate character set.

Because the Character pane displays the logical bytes rather than the physical bytes, the data in the Character pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.10.9 Binary Pane

The Binary pane displays the logical bytes in the frame in binary. This pane is synchronized with the Decode pane so that individual bit fields can be highlighted.

Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.10.10 Event Pane

The Event pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the All Events icon  .

Displaying all events means that special events, such as Start of Frame/End of Frame and any signal change events, are displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the Event Display window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.11 Protocol Layer Colors

7.1.11.1 Data Byte Color Notation

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the Decode pane is in the same

color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

7.1.11.2 Red Frame Numbers and Bytes

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

7.1.11.3 Changing Protocol Layer Colors

You can differentiate different protocol layers in the Decode, Event, Radix, Binary and Character panes.

1. Choose *Select Colors* from the Options menu to change the colors used
2. To change a color, click on the arrow next to each layer and select a new color.

7.1.12 Protocol Filtering from the Frame Display

7.1.12.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

7.1.12.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

7.1.12.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.

2. On the *Frame Display* window, click the starred *Quick Filtering* icon  or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

1. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.

2. Then click *OK*.

7.1.12.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display*  window.
2. Click the starred *Quick Filter* icon  or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

7.1.12.5 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

7.2 Protocol Navigator Window

7.2.1 Protocol Navigator

The *Protocol Navigator* displays the decode for more than one frame at a time, and has several features for controlling which frames and/or parts of frames are displayed. The main part of the window displays the decode for multiple frames. When you first open the window, every protocol layer of every frame is collapsed. By expanding the protocols, the

Protocol Navigator displays the equivalent of the *Decode* pane on the *Frame Display*, with the added convenience of displaying multiple frame decodes in one place.

Click the *Protocol Navigator* icon  to display the *Protocol Navigator*.

There are three methods for controlling the display in the *Protocol Navigator;* expanding/collapsing protocols, filtering, and hiding.

7.2.2 Protocol Navigator Toolbar

The buttons that appear in the Protocol Navigator window vary according to the particular configuration of the analyzer.

 Home – Brings the Control window to the front.

 Open File - Opens a capture file.

 I/O Settings - Opens the I/O Settings dialog.

 Start Capture - Begins data capture to a user designated file.

 Stop Capture - Closes a capture file and stops data capture to disk.

 Save - Save the currently selected bytes or the entire buffer to file.

 Clear- Discards the temporary file and clears the display.

 Event Display – Brings the Event Display window to the front.

 Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.

 Breakout Box - Opens the Breakout Box dialog.

 Duplicate View - Creates a second Frame Display window identical to the first.

 Apply/Modify Display Filters - Opens the Display Filter dialog.

 Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.


Find - Search for errors, string patterns, special events and more.


Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.


Add/Modify Bookmark - Add a new or modify an existing bookmark.


Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.


Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data


Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.


Packet Timeline – Opens the Packet Timeline display.


Extract Data - Opens the Extract Data dialog.


Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.


Audio Extraction - Opens the Audio Extraction dialog.


Network View - Opens the Network View Window.

Dashboard - Opens the Dashboard Dialog



The following icons all change how the panes are arranged on Protocol Navigator. Additional layouts are listed in the View menu.


First Frame - Moves to the first frame in the buffer.


Previous Frame - Moves to the previous frame in the buffer.


Next Frame - Moves to the next frame in the buffer.


Last Frame - Moves to the last frame in the buffer.

7.2.3 Protocol Navigator Status Bar

The Protocol Navigator Status bar appears at the bottom of the Protocol Navigator. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number(s) of selected (highlighted) frames, and the total number of selected frames in parentheses.

7.2.4 The Difference Between Filtering and Hiding

You can filter on one or more protocol layers. The filter is inclusive, which means that filtering on a protocol means that only frames that contain that protocol are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several. (Filtering on the Protocol Navigator window is display filtering only.)

Hiding means that the selected layer is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular layer by hiding every layer but the one of interest.

An example using the IP stack may help to illustrate the difference. Assume that you only want to see frames that have TCP in them. You create a filter on TCP. The results displayed in the Protocol Navigator (or Frame Display) window have only those frames that carry TCP.

Now you're ready to look at the TCP decode in your frames. You don't care about what has happened at the IP layer or any other layer, so you hide everything but TCP. The window shows just the TCP decode for each frame. With those two steps, you've eliminated looking at any frame that doesn't have TCP in it, and you've narrowed down what you see to just the TCP decode.

7.2.5 Hiding and Revealing Protocol Layers in the Protocol Navigator

Hiding means that the selected protocol is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular protocol by hiding every protocol but the one of interest. This is especially effective when all the layers are expanded.

Note: Hiding affects only the view in the Protocol Navigator  and not the view in any other window.

There are two ways to hide a protocol in the Protocol Navigator window :

1. Right-click on the protocol and choose Hide [Protocol Layer Name].
2. There are three panes on the left side of the window. The middle box is the Hidden From View pane. Check the boxes next to the protocols you want to hide.

To reveal a hidden protocol:

1. Right-click anywhere in the main window
2. Select the protocol you want to show from the right-click menu, or un-check the box next to the protocol name in the Hidden From View pane.

When one or more layers are hidden, a note appears at the top of the Protocol Navigator saying, "Some layers are hidden. Right-click to see." This warns you that some layers are hidden.

Two special options are *All But the Last Layer* and *All Special Information Nodes*.

- *All But the Last Layer* hides all layers in each frame except for the last one, regardless of which protocol is present in the last layer.
- *All Special Information Nodes* hides the information line present in some protocol decoders.

7.2.6 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

7.2.7 Filtering on all Frames with Errors from the Protocol Navigator

To filter on all frames with errors :

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

7.2.8 Expanding and Collapsing Protocol Layers

You can expand any collapsed frame or protocol layer by clicking on the plus sign next to the frame number or protocol name. Expanding a protocol layer in one frame expands it for all frames.

1. To collapse a layer or frame, click on the minus sign next to the frame number or protocol name.

What do you want to see?

Everything	Choose Show All from the Format menu.
Everything for just one frame	Click the plus sign next to the frame you want to see. Then click the plus signs next to each protocol name to see the full decode.
Just the stack for each frame	Choose Show Frames AND Show Protocol Stack When Frame Is Completely Collapsed from the Format menu. This makes the display look similar to the following:

Frame 1: Len=104 Ethernet -> IP -> TCP

Frame 2: Len=98 Ethernet -> IP -> TCP -> NBSS

Just the stack without summary information Choose Show Layers AND un-check Show Summary Decode When Detailed Decode Is Collapsed on the Format menu. This makes the display look similar to the following:

Frame 1: Len=104
+ Ethernet:
+ IPv4:
+ TCP:

Frame 2: Len=98
+ Ethernet:
+ IPv4:
+ TCP:
+ NBSS:

Just the stack including summary information Choose Show Layers AND Show Summary Decode When Detailed Decode Is Collapsed from the Format menu. This makes the display look similar to the following:

Frame 1: Len=104
+ Ethernet: --- Dest. Address: BROADCAST Source Address: XYZ etc.
+ IPv4: --- Protocol: TCP Length: 80 etc.

+ TCP: --- Source Port: 9988 Destination Port: NETBIOS etc.

Frame 2: Len=98

+ Ethernet: --- Dest. Address: etc.

+ IPv4: --- Protocol: TCP Length: 56 etc.

+ TCP: --- Source Port: NETBIOS Destination Port: 9988 etc.

+ NBSS: --- Length: 23 Fragment: Entire Message

The full decode for a protocol layer	Click on the plus sign next to the protocol name. This expands just that protocol in every frame.
The decode for just the last layer in each frame	Choose Collapse All Nodes AND Show Last Layer When Frame is Completely Collapsed from the Tree menu.

8 Analyzing Control Signal Changes

8.1 Viewing Signal Changes in Real-time

8.1.1 Breakout Box Window

The Breakout Box window provides a real-time graphical view of control signals. The window is customizable based on the control signals you wish to view and your preference of indicators (+/-, 1/0, T/F, arrows, and simulated LEDs). Also included are counters showing the number of times a control signal has changed.

To open this window :

1. Click the Breakout Box icon  on the Control window.

Name - Pin 1, 2, 3, and 4

FTS4USB monitors four control signals.

Digital inputs provide a means for users to insert events into the data stream. There are four digital inputs that can be enabled individually. Whenever an enabled input changes state it will issue an event and be tagged with a timestamp of when the input was interpreted by the analyzer. Digital inputs can not exceed a rate of 30 MHz. Digital inputs that occur faster than that are not guaranteed to be interpreted correctly by the analyzer. Also, only one digital input event may occur per active packet. All other digital input events can only be handled after the packet has completed. Digital inputs, although guaranteed to have the correct timestamp given the previous conditions, have the possibility of being presented out of order because they are provided randomly by the user and have no direct correlation to the bus. It is important to note that the digital inputs are susceptible to cross-talk if they are not being actively driven. A situation like this could occur if a digital input has been enabled, but has not been tied to a signal. Any other nearby signal (i.e., other digital inputs or outputs) could cause the input to activate. It is recommended that all undriven digital inputs be disabled or tied to ground.

FTS monitors six *RS-232* control signals. They are listed below :

DTE Signals

- *DTR - Data Terminal Ready*
- *RTS - Request to Send DCE Signals*
- *CTS - Clear to Send*
- *DSR - Data Set Ready*
- *CD - Carrier Detect*
- *RI - Ring Indicator* (see the special note on capturing Ring Indicator changes)

When monitoring a synchronous circuit, FTS also displays clock signals at the bottom of the window. These signals rotates when clock is present, and has an X over them if clock is not detected.

When using the SST interface cards for analyzing DeviceNet traffic, the following signals are displayed:

- BP - Bus Power
- OL - Online
- BW - Bus warning, either the receive or transmit error counter (incremented and decremented at various rates according to the Bosch CAN specification) has reached 128.
- BO - Bus off, either the receive or transmit error counter has reached 255 and the CAN chip has been forced offline.
- RO - Receive buffer overrun, one or more messages has been lost due to a full queue in the on-card firmware.
- ML - Message lost, one or more messages has been lost due to a slow interrupt response by the on-card firmware.
- ER - Error, one or more CAN error frames has been detected.

Note: The messages received by NetDecoder are still correct when the ER flag shows some activity, as re-transmission is automatic and only error-free frames result in a receive interrupt from the CAN controller.

8.1.2 The Breakout Box Toolbar



Home - brings the Control window to the front.



Reset - resets the Breakout Box window.



Lock - Locks the display. Clicking on the Lock icon, unlocks the window.



Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon, locks the window.



Options - Brings up the Breakout Box Options window. This window allows you to change the window refresh rate and choose which control signals to display. Type topic text here.

8.1.3 Reading the Breakout Box Window

The Breakout Box display is divided into three main parts. The first part (to the far left of the screen) shows the abbreviated name of the control signal being monitored. These names can be changed in the I/O Settings window  by clicking the *Names* button.

The second part shows the control signal counters. The counters show how many times each control signal has changed state. This is useful in situations when signals may be changing state too rapidly to be displayed graphically.

Below the counters are the clock indicators. The indicators rotate when clock is present, and have an X over them when clock is not detected.

The third part of the Breakout Box shows the current states of the control signals. The indicators show the state that the control signal is currently in, and the line graph displays the state of the signal over time. A single line means that the signal is logically off, while a double line means that the signal is logically on. A half-height "tick" means that a signal has gone through one full transition (from off to on to off, or vice versa) since the analyzer last updated the screen.

To change the indicators, hide the clock signals, or change the rate at which the analyzer updates the window, click on the Options icon  .

8.1.4 Selecting Breakout Box Options

To access options

1. Click the Options icon  on the Breakout Box toolbar or choose *Breakout Box options* under the *Options* menu.

Display Signal

This box shows which control signals FTS monitors.

- A check mark next to a control signal name indicates that the breakout box displays the status of that control signal.
- To prevent FTS from displaying the status of a signal, un-check the box next to it.

Display Clocks

Click to place a check mark in this box if you want the Breakout Box window to display the clock indicators. Un-check to hide the clock indicators. (This option is only shown when in synchronous or isochronous mode.)

Window Refresh Rate

The refresh rate is the rate at which FTS updates the window.

- By default, FTS refreshes the display once every 1,000 milliseconds (one second.)
- To change the rate, highlight the number in the box and enter a new number. See item 7 in Performance Notes for information on how Window Refresh Rate can affect performance.

Indicators

You can choose what type of indicators FTS uses.

- The default indicators are a green "+" sign to show a logically high state, and a red "-" sign to show a logically low state.
- To change the indicators, click on the down arrow and choose a pair of indicators from the list.
- As a reminder, FTS gives the definition of the indicators in the top part of the Breakout Box window.

9 Viewing Historical Signal Changes

9.1 Signal Display Window

The Signal Display window provides a graphical view of control signal transitions that you can manipulate. You can zoom in to view the state of control signals for a range of events, or zoom out to view control signal changes over the course of an entire capture session.

To open this window

Click the Signal Display icon  on the Control window toolbar, or choose Signal Display from the Window menu.

The Signal Display window does not provide a real-time view of control signal changes. It is intended to be used as a post-process review screen. Use the Breakout Box window to view real-time control signal changes. Note that if you bring up the Signal Display window while data is being captured, the window shows you the state of the control signals at the time the window was opened. This is called a "snapshot" because it is a picture of the buffer at the time the Signal Display was opened. To update the display to reflect the current state of the buffer, use the New Snapshot icon  .

When you open Signal Display IN FTS4USB you will see Pin Codes 1, 2, 3, and 4. These correspond to the four Digital Input Enabling Options explained in USB I/O Settings.

When using the SST interface cards for analyzing DeviceNet traffic, the following signals are displayed:

- BP - Bus Power
- OL - Online
- BW - Bus warning, either the receive or transmit error counter (incremented and decremented at various rates according to the Bosch CAN specification) has reached 128.
- BO - Bus off, either the receive or transmit error counter has reached 255 and the CAN chip has been forced offline.
- RO - Receive buffer overrun, one or more messages has been lost due to a full queue in the on-card firmware.
- ML - Message lost, one or more messages has been lost due to a slow interrupt response by the on-card firmware.
- ER - Error, one or more CAN error frames has been detected.

Note: The messages received by NetDecoder are still correct when the ER flag shows some activity, as re-transmission is automatic and only error-free frames result in a receive interrupt from the CAN controller.

9.2 Signal Display Toolbar



Home - brings the Control window to the front.



Take New Snapshot - Takes a new "picture" of the capture buffer. If you are capturing data when you open the Signal Display window, the window shows only the state of the control signals that were in the buffer when the window was opened. Click this button to update the window with the contents of the current buffer.



Zoom In - "Zooms in" on the signal display. How much you zoom in is determined by your selection in the Signals menu. You can zoom in by a factor of 2, 4, or 8.



Zoom Out - Reverse of Zoom In.



Zoom to Selection - Zooms to show only the region highlighted on the screen. If the highlighted area contains few events, the Signal Display window may also display additional events in order to fill up the screen.



Display Entire Buffer - Zooms all the way out to display the contents of the entire buffer in the window.



Find - Opens the Find Control Signal change window.



Snap to Nearest Change - Moves the cursor to the nearest signal change whenever you click on the line graphics in the window. Find the line for the control signal whose changes you want to see. Click on that line, and the analyzer moves to the nearest signal change for that control signal. You can also highlight a range, and the analyzer snaps to the 2 nearest changes on either side of the range.



Timestamping Options - Opens the Timestamping Options window, where you can change the timestamping resolution and how timestamps are displayed.

9.3 Reading the Signal Display

Control signal changes are displayed in a graphical format. On the left side of the screen is a list of the signals currently being displayed, and to the right of each name is a line displaying the state of the signal over time. A single line means that the signal was logically off, while a double line means that the signal was logically on. Dotted lines are used for signals that were not present at the time of capture. For example, if you are monitoring a circuit that does not use CD, that line appears as a dotted line in the control signal display.

The four information lines at the bottom of the window tell you what events are being shown in the window, and where you are in relation to the buffer as a whole.

- The first line tells you what event numbers are in the current snapshot, the total number of events, and the amount of time that passed between the first event in the snapshot and the last event (called Delta).
- The second line gives the same information about the events that are currently visible in the window. Because you can zoom in and out, often the events being shown in the window are not the same as the number of events in the current snapshot.
- The third line gives the same information for the currently selected events. You can highlight a range of events by clicking at any point on the graphical display and dragging the mouse to the left or the right. The third line shows information for the selected range.
- The fourth and last line shows the exact timestamps of the first and last bytes in the currently selected range. Note that this does not tell you the timestamp for the entire snapshot or the events displayed in the window, just the highlighted events.

A single mouse click places the cursor in the window. The analyzer highlights all six signal changes in one color, and uses a different color to specify the control signal line clicked on. You can highlight a range by clicking and dragging the mouse to the right or left. You can also use the arrow keys to move the cursor to the right or left.

The Signal Display window is synchronized with other windows in the analyzer. A range highlighted in the Signal Display window is also highlighted in the Event Display and Frame Display windows.

The Snap to Nearest Change icon  lets you place the cursor on the signal change you want to look at without needing to click on exactly the right spot. Find the line corresponding to the control signal you want to look at. Click on the line, and the analyzer moves the cursor to the nearest change. If you highlight a range, the analyzer "snaps to" the nearest changes on either side. This feature is active when the Snap To button is pressed, and inactive when the button is not pressed.

Use the Zoom In and Zoom Out buttons to increase and decrease the magnification of the window. The analyzer changes the magnification by a factor of 2, 4 or 8, depending on the option selected in the Signals menu.

If you want to see a range in greater detail, highlight the range you want to view and click on the Zoom to Selection icon  . The analyzer zooms in to show only that range in the window. If the range is small, the analyzer may add additional events to fill up the window.

To view the entire snapshot in the window, click on the Display Entire Buffer icon  .

Note that if you bring up the Signal Display window while data is being captured, the window shows you the state of the control signals at the time the window was opened. To update the display, use the New Snapshot icon  .

9.4 Selecting Signal Display Options

To access Signal Display Options

Click the Signal Display icon  on the Control window toolbar. From the *Options* menu, select Signal Display Options.

To choose which control signals to display in the Signal Display window.

- Click on a box to check or un-check it the control signal name.
- A check mark next to a control signal name means that the signal is displayed.

10 Statistics

10.1 Statistics

Statistics displays vary according product configuration. Select the help topics that apply to the mode you are running.

Serial and USB Statistics

Air Sniffer Statistics

10.2 Statistics Window

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

To open the Statistics window, click the Statistics icon  on the Control window toolbar, or choose Statistics from the View menu on the Control window.

The Statistics window supplies basic information about the data on the network. When reviewing a capture file, the Statistics window shows a summary of the data in the file.

The analyzer monitors the network and collects statistics all the time, even when data is not actively being captured. Activate the Lock icon  to stop the window from updating.

Click the Unlock icon  again to resume updating. The analyzer continues to monitor network traffic while the Statistics window is locked, so you may see the numbers jump right after updating has resumed, reflecting all the statistics that were gathered while the window was locked.

10.3 Session, Resettable and Capture File Tabs

The Session and Resettable tabs are parts of the Statistics window.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Information about all data collected since the analyzer was started is shown in the Session tab. The Session tab cannot be reset; in this sense, it is like the odometer on a car. The odometer on a car shows you all the miles driven since the car was built, and the Session tab shows you all the data collected since the analyzer was started.

If you think of the Session tab as the odometer, then the Resettable tab is the trip odometer. It can be reset, and allows you to record statistics for a new "trip". In this way you can effectively start a new session without having to restart the analyzer. If the Reset button was pressed during the capture, then the numbers on this tab differs from the numbers on the Session tab.

The Capture File tab shows information on the data that is currently in the capture. If the capture file had become full, the analyzer began to overwrite the oldest data and put new data in its place. This is called "wrapping". If the file wrapped, the numbers on the Capture File tab is smaller than those on the Session tab.

Occasionally some of the statistics read n/a, for Not Available. This happens for various reasons. For example, many of the items on the Capture File tab become not available (n/a) if the buffer becomes full and wraps. When this happens, the analyzer can no longer provide accurate statistics for the data in the file, because some of the data that the statistics are based on has been lost.

10.4 Copying Statistics To The Clipboard

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

To copy the information from an individual table to the clipboard (where it can be pasted into any application),

1. Choose the name of the table from the *Edit* menu.
2. To copy the contents of all the tables, choose *Copy All to Clipboard*.

10.5 Graphs

10.5.1 Statistics Graphs

Open the Statistics window and click on the picture of a graph  on the table header, or choose the graph name from the Graph menu on the Statistics window.

The Frame Sizes Graph window has Session, Resettable and Buffer tabs that correspond to the tabs on the Statistics window. Each tab shows the data that corresponds to the appropriate tab on the Statistics window.

The Frame Sizes Graph window displays the number of frames of each length in either a pie chart or bar graph format. Click the Pie icon  to display a pie chart, and click the Bar icon  to display a bar graph.

For networks with more than one side, the analyzer displays one graph for each side. To view the aggregate of all sides, click the Aggregate icon  .

10.5.2 Printing Graphs

1. Click the Print icon  to print the graph. The analyzer prints exactly what is shown on the window.

10.5.3 Changing the Graph Refresh Rate

The graphs window refreshes once every second.

To change the refresh rate:

1. Click the Options icon  on the *Statistics* window.
2. Enter a new refresh rate in milliseconds in the Time Interval (ms) text box.

10.5.4 Viewing Percentages or Values

On the *Statistics* window you can view data expressed as a percentage.

1. Open the *Statistics* window
2. Select the graph to display.

On the graph window,

3. Click the *Percentages* icon  to view data expressed as a percentage.
4. Click the *Percentages* icon again to view the actual number of items of each type.
5. Click the *Show Data Grid* icon  to view both the number and percentage of the total for each item. The analyzer places a grid in the legend.

10.6Information on Tables

10.6.1 Statistics Tables

The Statistics Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

The information on the Statistics window is organized into Tables. Fields marked "n/a" are fields for which there is currently no data. This can happen for a variety of reasons. On the buffer tab, fields are n/a when there is no data in the buffer (i.e. no capturing is being done). On the Errors table, some fields may be n/a depending on the statistics supported by your Ethernet card. Some tables are always present, while tables with framing information are present only when capturing framed data.

10.6.2 Bytes Per Second Table

The information in the Bytes Per Second table is recorded while running an Ethernet analysis.

Speed The maximum speed of the network expressed in megabits

Current The current number of bytes per second.

Average The average number of bytes per second.

Peak The highest number of bytes per second.

10.6.3 Frames Per Second Table

The Frames Per Second Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of frames per second.

Average The average number of frames per second.

Peak The highest number of frames per second.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

10.6.4 Characters Per Second Table

The Characters/Sec Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Baud The current baud.

Current The current number of characters per second.

Average The average number of characters per second.

Peak The highest number of characters per second.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

10.6.5 Utilization Table

The Utilization Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Average The average number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Peak The highest utilization.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

10.6.6 Data Table

The Data Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

The information in the Data table relates to the amount of data captured by the analyzer. Data information varies depending on the type of data in the capture. When Ethernet data passes through a capture filter, this table displays statistics only for the data kept by FTS, i.e. only the data that passes the filter. The Unfiltered Data table always displays statistics for the entire network, regardless of the state of any capture filter.

Ethernet Data

Frames This includes frames received with and without errors, and frames transmitted by the PC running the analyzer, if the PC is an active node on the network. This field and the Total Frames field in the Unfiltered Data table should be roughly equal, unless a capture filter is active. They are not exactly equal because the counters are updated at different times.

Bytes The total number of bytes.

Events The total number of events captured. Events include data bytes and start-of-frame and end-of-frame markers. For a description of all events and their symbols, see the List of Event Symbols.

Multicast The total number of multicast frames.

Broadcast The total number of broadcast frames.

Serial Data

Frames The total number of frames, if applicable, with a breakdown by DTE and DCE device.

Chars The total number of characters, with a breakdown by DTE and DCE device.

Events The total number of events captured. Events include data bytes, control signal changes, flow control changes, etc. For a description of all events and their symbols, see the List of Event Symbols.

Wireless Data

Frames The total number of frames, if applicable, with a breakdown by device.

Octets The total number of octets, with a breakdown by device.

Events The total number of events captured. Events include data bytes, start and end-of-frame markers, etc. For a description of all events and their symbols, see the List of Event Symbols.

10.6.7 Unfiltered Data Table

The information in the Unfiltered Data table is recorded by NDIS while running an Ethernet analysis. Some NDIS drivers may not report all of the statistics on this table, in which case the field lists an n/a. This table always reflects the total amount of data on the network.

Rx Frames W/O Errors The total number of frames received with no errors.

Tx Frames W/O Errors The total number of frames transmitted by the NIC with no errors.

Total Frames The total number of frames, including frames with errors. This field and the Frames field on the Data table should be roughly equal, unless a capture filter is active. They are exactly equal because the counters are updated at different times.

Bytes The total number of bytes.

Multicast Frames The total number of multicast frames.

Broadcast Frames The total number of broadcast frames.

10.6.8 Octets Per Second Table

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)

- USB HCI

Speed maximum speed of the network expressed in megabits

Current current number of octets per second

Average average number of octets per second

Peak highest number of octets per second

10.6.9 Buffer Information Table

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

These errors do not indicate problems on the network, but rather indicate that FTS was not able to keep up with the amount of incoming data. They usually indicate that a faster PC was needed. See Performance Notes for more information.

Driver Buffer Overflow The number of times the analyzer lost frames because it could not retrieve them from the driver buffer fast enough.

The remaining three items are for Ethernet data only.

Frames Missed, No Buffer The number of frames lost because the analyzer driver could not retrieve them from the NDIS buffers before they were overwritten by new, incoming frames.

Receive Overrun The number of times that frames are lost because NDIS could not retrieve data quickly enough from the buffer on the network card.

Frames Lost The number of frames lost due to driver buffer overflows.

Errors Table

The Errors Table is found on the Statistics window. The table provides the number of each type of error seen on the network. Error types vary depending on the type of data. When analyzing Ethernet data, not all errors are supported by all NDIS drivers. Errors not supported are marked "n/a".

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- Serial Asynchronous
- High Speed Serial HCI
- High Speed UART (HSU)

To graph, click the bar graph icon  on the Errors table header.

Ethernet Errors

CRC Errors	The number of frames with *CRC* errors. A CRC error occurs when the frame is properly aligned on a byte boundary but does not pass the Cyclic Redundancy Check. The CRC verifies that the data was not corrupted in transit.
Alignment Errors	The number of frames with alignment errors. Alignment errors occur when the frame does not end on a byte boundary. For example, frames may not be 95 and 2 bits long. It must be either 92 or 93 bytes.
Rx Frames With Errors	The total number of frames received with errors (includes frames with CRC and Alignment errors).
Tx Frames With Errors	The total number of frames transmitted with errors.
Tx One Collision	The number of frames successfully transmitted after detecting one collision.
Tx More Collisions	The number of frames successfully transmitted after detecting multiple collisions.
Tx Deferred	The number of frames successfully transmitted after transmission has been deferred at least once.
Tx Max Collisions	The number of frames not transmitted due to excessive collisions.
Tx Underrun	The number of frames not transmitted due to underrun errors.
Tx Heartbeat Failure	The number of frames transmitted without detecting the collision detection heartbeat.

Tx Times CRS Lost The number of times carrier sense was lost during frame transmission.

Tx Late Collisions The number of collisions detected after the normal window.

Serial Asynchronous Errors

Overrun The number of overrun errors broken down by DTE and DCE device.

Parity The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.

Framing The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.

Serial Synchronous Errors

USART Overrun The number of overrun errors broken down by DTE and DCE device.

Parity The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.

Framing The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.

CRC The number of *CRC* errors detected. CRC counting is done only when monitoring HDLC or SDLC data.

Underrun The number of underrun errors broken down by DTE and DCE device. Underrun errors occur when FTS is unable to transmit data quickly enough. These errors only occur when transmitting in sync mode.

High Speed Serial HCI and High Speed UART (HSU) Errors

Parity The number of parity errors broken down by device.

Framing The number of framing errors broken down by device.

ZigBee Errors

FCS The number of FCS errors detected.

10.7 Packet Error Rate Statistics (PER Stats)

10.7.1 Packet Error Rate

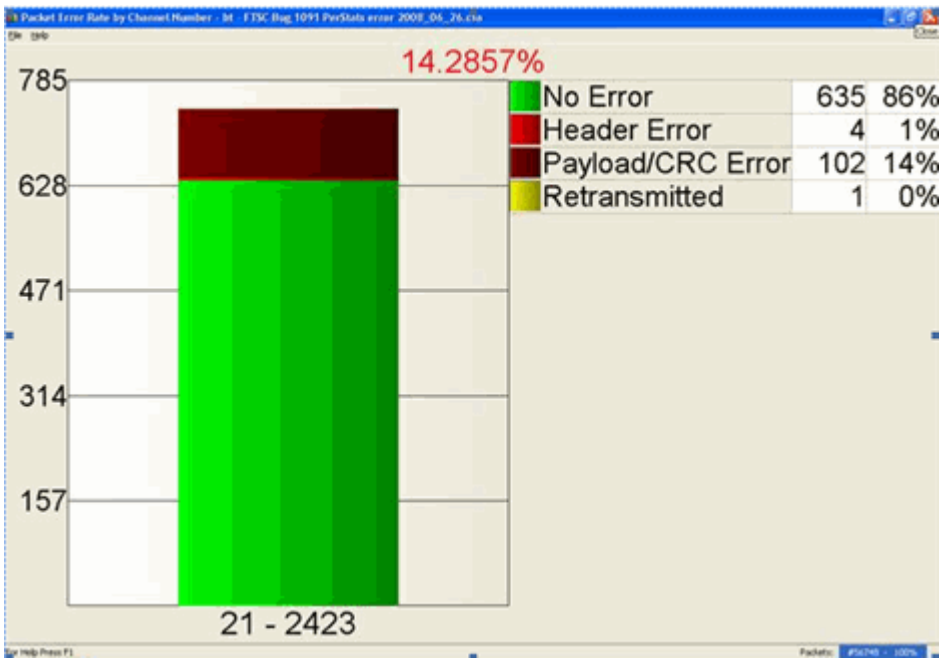
The Packet Error Rate Stats Plug-in provides a dynamic graphical representation of the Packet Error Rate for each channel.

The Packet Error Rate window displays a graph for each channel numbered 0 through 78 and a pie chart summarizing the total of all channels.

Expand individual graphs by clicking on the desired one. The expanded graph displays the percentage of errors (Packet + Header if any) in red text at the top of the graph, and a legend with color-coded statistics in percentages and actual values, by parameter, in tabular format, to the right of the graph. Click the expanded graph to return to the Packet Error Rate window.

Each graph and table display the following parameters:

- Total number of packets (determined by reading the scale to the left of the graph)
- The number of packets with no errors, color-coded green
- The number of packets that have header errors, color-coded red
- The number of payload errors, color-coded dark red
- The number of re-transmits, color-coded yellow



Click on the error rate percentages in the graphic above to learn more about the Packet Error Rate percentages.

The Reset button is available only during live capture and not when viewing a capture file. It resets the Packet Error Rate Stats display to all zeros, and starts displaying data from that point on.

Unavailable channels, due to Adaptive Frequency Hopping (AFH), display the "not" symbol. However, the graph may contain data against transmissions made prior to becoming unavailable.

Data Analysis

Packet Error Rate Stats assist in detecting bad communication connections. When a high percentage of re-transmits, and/or header/payload errors occur, careful analysis of the statistics indicate whether the two devices under test are experiencing trouble communicating, or the packet sniffer is having difficulty listening.

Generally, if the statistics display either a large number of re-transmits with few errors or an equal number of errors and re-transmits, then the two devices are not communicating clearly. However, if the statistics display a large number of errors and a small number of re-transmits, then the packet sniffer is not receiving the transmissions clearly.

Note: The total percentage of the Packet Error Rate can be < or > 100%. The discrepancy can be attributed to the rounding methodology. For example, look at the following numeric values and the resulting rounded values:

- 635/742 = 0.8557 -> 86%
- 4/742 = 0.0053 -> 1%
- 102/742 = 0.1374 -> 14%
- 1/742 = 0.0013 -> 0%

Note that a count of 1 is shown as 0% because the actual percentage rate is 0.0013. 1 is an actual value, but rounding gives it a percentage of 0. Also note that 4 is rounded to 1% even though the actual percentage is 0.0053.

What you can have, then, is a total percentage of 101% and still be correct. You could also have a total percentage of 99% and be correct.

The total percentage of the Packet Error Rate can be < or > 100%. The discrepancy can be attributed to the rounding methodology. For example, look at the following numeric values and the resulting rounded values:

- 635/742 = 0.8557 -> 86%
- 4/742 = 0.0053 -> 1%
- 102/742 = 0.1374 -> 14%
- 1/742 = 0.0013 -> 0%

Note that a count of 1 is shown as 0% because the actual percentage rate is 0.0013. 1 is an actual value, but rounding gives it a percentage of 0. Also note that 4 is rounded to 1% even though the actual percentage is 0.0053.

What you can have, then, is a total percentage 0f 99% or 101% and still be correct.

10.8 Data Highway Plus Statistics

Frontline Test Equipment's DH+ product includes powerful statistical analysis capabilities. Easily accessible and up to date statistical data provides the user with valuable information when starting up, surveying, benchmarking, and troubleshooting DH+ networks.

DH+ stats runs automatically when a capture file is loaded or when a live capture is performed and cannot be turned off. All of its dialogs can be brought down, however.

Driver buffer overflows and UART overruns during live capture cause data loss that can result in some invalid frames. This can affect the values shown in DH+ Stats. To prevent driver buffer overflows, try increasing "Driver Receive Buffer Size in Operating System Pages" in "Options : System Settings : Advanced". To prevent UART overruns, try running on a faster machine. Driver buffer overflows and UART overruns are also displayed on the regular Statistics screen, accessible from the Control dialog via "View : Statistics".

10.8.1 Starting DH+ Statistics

DH+ Statistics is started from the NetDecoder application. DH+ Stats should launch automatically when the application is started. However, if it does not start automatically, then follow the steps below.

Launch NetDecoder Protocol Analyzer for DH+, and perform the following:

1. From the *File* menu on the *Control Window.*, open the desired capture file
2. The system should display the *DH+ Overview* dialog.
3. If the dialog does not appear, then open the *View* menu on the *Control Window.*
4. Select *DH+ Statistics.*

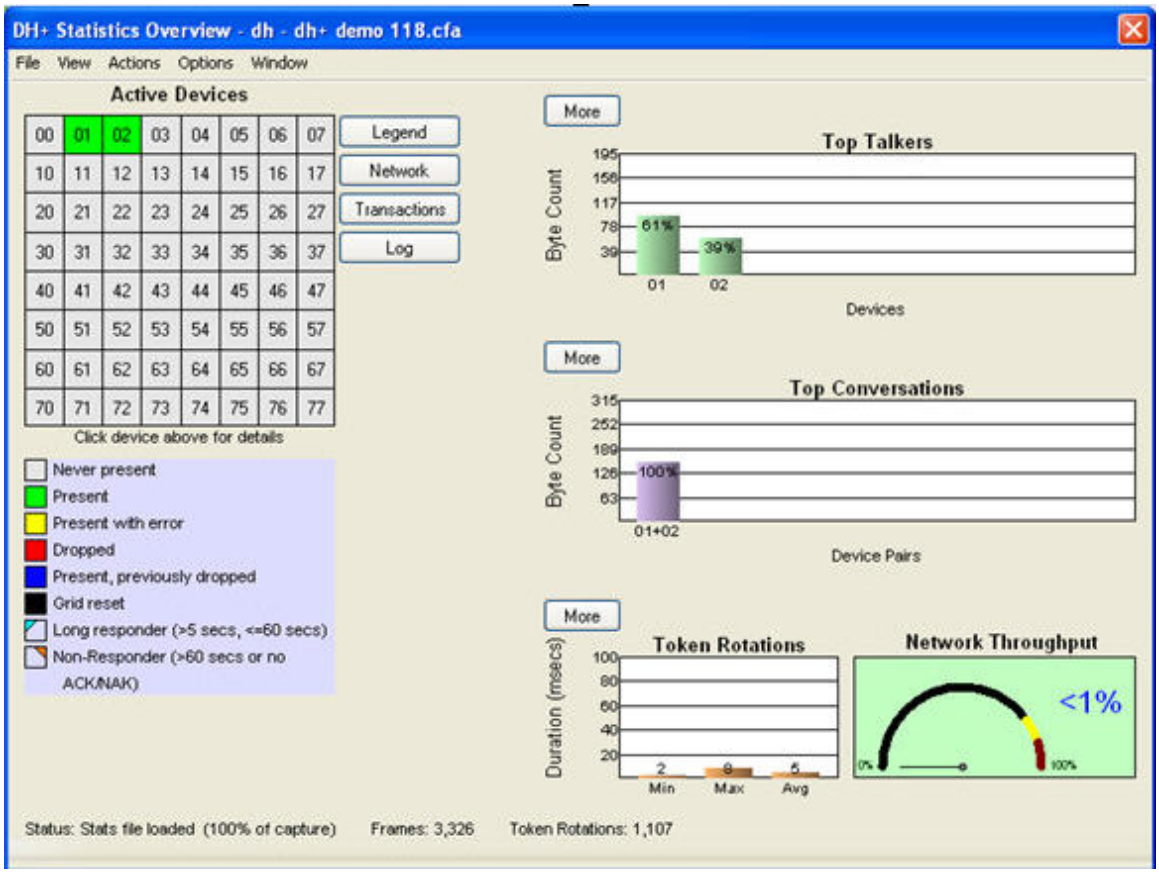
10.8.2 Overview Dialog

The DH+ Statistics Overview screen displays key information pertaining to the overall health of the network in tabular format, as well as an Active Devices grid that identifies all the devices currently on the network.

The three table displays on the overview screen provide the user with current statistical information on Top Talkers, Top Conversations and Token Rotation Times. The overview screen affords the user easy access to detailed information on individual devices, graphs of statistical data, and statistics on Network Bytes Sent, Transactions Summary, and a Network Event Log. The Overview dialog is the main dialog. All other dialogs are reached either directly or indirectly from this dialog.

DH+ Statistics provides powerful network monitoring capabilities. For this reason, the Overview dialog displays statistical data updated in real-time, as do all dialogs in DH+ Statistics.

The Active Devices grid appears in the upper-left corner of the dialog. This simplifies network monitoring by allowing the user to drag the Overview dialog to the lower right-hand corner of the computer screen hiding all but the Active Devices grid and the Synopsis information.



10.8.2.1 Active Devices Grid

The Active Devices grid appears on the Statistics Overview dialog. This grid is a color-coded 8x8 grid that shows the current status of each *device*. Clicking on a device square in the grid brings up the Device Transactions dialog for that device. A colored square is used for conditions where the device is or has been present. A triangle in the upper-right corner of a square is used for conditions where the device may never have been present.

The Active Devices Grid color code is as follows:

- Gray: Device never present
- Green: Device present and OK

- Yellow: Device present with at least one error *
- Red: Device absent (dropped off bus)
- Blue: Device present, previously dropped off bus (supercedes yellow)
- Black: (Optional) Device has not reappeared after grid reset
- Cyan Triangle: A long-responder takes between 5 seconds and 60 seconds to respond
- Orange Triangle: A non-responder takes more than 60 seconds to respond or no immediate ACK/NAK

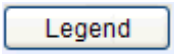
Footnotes:

* A device can have the following "condition yellow" errors:

- Sent *NAK* to a *Command* or *Reply*.
- Had error in decode or summary panes of Frame Display.
- Sent a *Token*, *Solicit*, Command, or Reply but wasn't the token holder.
- Sent *ACK* or NAK but hadn't received a Command or Reply.
- Sent to an invalid (out of range) device number.
- Sent to itself.

10.8.2.2 Active Devices Grid Buttons

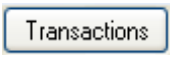
These buttons, located to the right of the Active Devices Grid on the Statistics Overview window initiate the following displays:



Displays the help topic for the Active Devices Grid



Displays the Network Bytes Sent dialog



Displays the Transactions Summary dialog



Displays the Network Event Log dialog

With the exception of the grid, numbers of devices that have never been present are enclosed in double parentheses, and numbers of devices that are currently absent but have been present are enclosed in single parentheses.

Driver buffer overflows and UART overruns (both shown on the regular Statistics screen, reachable via "Control Window: View : Statistics") during live capture cause data loss that can result in some invalid frames. This can affect the values shown in DH+ Stats. To

prevent driver buffer overflows, try increasing "Driver Receive Buffer Size in Operating System Pages" in "Control Window : Options: System Settings : Advanced". To prevent UART overruns, try running on a faster machine. For further assistance please contact Technical Support.

10.8.2.3 Status

Status appears just below the Synopsis.

Status can display the following:

- **Capturing to file:**
  Displayed during a live capture to file
- **Done capturing to file:**
  Displayed when a live capture to file finishes
- **Reading capture file:**
  Displayed when the capture file is first opened, before displaying any statistics
- **Reading capture file (n%):**
  Displayed when there are statistics displayed for one or more frames. This indicates how much of the capture file has been processed by the plugin
- **Done reading capture file:**
  Displayed when a capture file has been fully read
- **Loading stats file:**
  Displayed while a statistics file is being loaded
- **Stats file loaded (n% of capture):**
  Displayed when a statistics file is fully loaded. The "n%" is the percentage of the capture file's frames that were sent to DH+ Stats (some of which may have been missed by DH+ Stats).
- **Unable to load stats file:**
  Displayed when a statistics file cannot be loaded. Usually caused by an obsolete version number contained in the statistics file.
- **Exiting:**
  Displayed when DH+ Stats is being terminated. This status usually appears for just an instant.

10.8.2.4 Top Talkers Chart

The *Top Talkers* chart appears in the top right portion of the DH+ Statistics Overview dialog.

- The Top Talkers display sorts the *device* list by *Byte Count* , allowing the user to identify which devices use most of the available network bandwidth.
- The calculated statistics displayed in the Top Talkers table include data only from *Command* and *Reply* messages, and does not include data from required protocol messages (*ACK*, *NAK*, *Token* and *Solicit*).

Selecting the *More* button displays the Top Talkers Dialog, which displays both a graph and a table.

10.8.2.5 Top Conversations Chart

The *Top Conversations* information table appears in the middle right portion of the DH+ Statistics Overview dialog.

- The Top Conversations statistic sorts the *device* list by *Byte Count*, allowing the user to quickly identify which pair of devices generate the most *traffic* on the network.
- The statistics displayed in the Top Conversations table includes data only from *Command* and *Reply* messages, and does not include data from required protocol messages (*ACK*, *NAK*, *Token* and *Solicit*).

Selecting the *More* button displays the Top Conversations Dialog which displays both a graph and a table.

10.8.2.6 Token Rotations Summary Chart

The *Token Rotation* Summary information table appears across the bottom portion of the DH+ Statistics Overview dialog. This table contains information about the Token Rotation Times, including minimum, maximum, average and current values. Token Rotation Times directly relate to network performance. The values in the summary table are an indicator of system throughput and performance. DH+ Statistics calculates and displays actual response times on the individual Device Transaction dialog as well as the Transaction Summary dialog.

The measured Token Rotation Time for each of the four indicators (minimum, maximum, average, and current) appears in the Duration column. Typically, a complete Token Rotation starts when a Token passes from a higher device ID number to a lower device ID number. Then it passes up through incrementing device ID numbers. When the highest active ID numbered device obtains the Token and passes it to a lower device ID number, the Token Rotation ends and the next one begins.

Selecting the *More* button displays the Token Rotations dialog which displays both a graph and a table.

10.8.2.7 Network Throughput

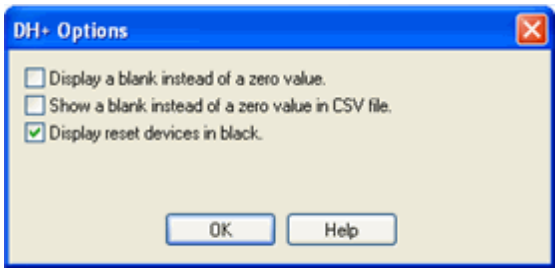
Network Throughput displays the percentage of network traffic being used.

10.8.2.8 Setting Display Options

Display Options selections affect how statistics data is displayed, not how it is stored by DH+ Statistics.

To access the Display Options dialog:

1. Select *Options* from the Options menu on the *Overview* dialog, and the system displays the *DH+ Options* dialog


DH+ Options
Display a blank instead of a zero value.
Show a blank instead of a zero value in CSV file.
Display reset devices in black.
OK
Help

2. Add or remove the desired display options using the check boxes
3. Click the *OK* button to apply the display options

The *Display Options* dialog closes, and applies the selected options

Display Options definitions:

Display a blank instead of a zero value:

Default Value: Unchecked

Statistical data is often displayed in tabular format. DH+ Statistics stores a value for each cell in these tables. If there is no value for a particular cell, then the system stores a value of zero. Some tables may contain many cells with a zero value, and when these tables are displayed, they may appear cluttered and hard to read. Selecting this option changes the table displays to hide zeros in the cells that contain only a zero value.

Show a blank instead of a zero value in CSV file:

Default Value: Unchecked

This option hides the zeros in cells that contain a zero value in a CSV file in the same way that the "Display a blank instead of a zero value" does in the tables.

Display reset devices in black:

Default Value: Checked

This option affects the Active Devices grid display. DH+ Statistics is equipped with a means to reset all of the colors displayed in the active devices grid to Gray. This option allows the user to reset previously active devices to display in black instead of gray. This separates those devices from the ones in the grid that were never active.

10.8.3 Individual Device Statistics

10.8.3.1 Device Transactions Dialog

The *Device Transactions* dialog shows transaction statistics for a selected device.

Access this dialog by clicking on the desired device number in the Active Devices grid on the *Overview* dialog. A transaction is a sequence of messages consisting of a *Command* followed by a *Reply*, with an *ACK* or *NAK* after each one, as follows:

1. Device A sends a Command to device B.
2. Device B sends an ACK or NAK to device A.
3. If device B sent an ACK, it then sends a Reply to device A.
4. Device A sends an ACK or NAK to device B.

The Device Transactions dialog provides detailed statistics on all *traffic* to and from the selected device. This dialog lists the conversation types on the left side, and displays the statistics for each in the adjacent table. The list items contain both the message type (Commands, Replies, ACKS, NAKS) and the associated action (Sent to, Received from). In addition, the table contains statistics on device response times. Response time statistics used in conjunction with statistics from other devices assist in identifying worst-case conditions.

The top table displays statistics for traffic originating from the selected device. Conversely, the bottom table displays statistics for traffic originated by other devices and directed toward the selected device.

On a well-behaved network with no errors, the numbers of Commands, Command ACKs, Replies, and Reply ACKs are all equal. These numbers can be unequal in the table due to many factors, including transmission noise, partial *token* rotations discarded by DH+ Stats (this is normal behavior), un-captured frames (frames that occurred before or after the capture session), frames missed by DH+ Stats, and absent devices. To determine whether network or device errors have occurred, consult either the Network Event Log or the Active Devices grid (look for a device box that is yellow, red, or blue, or has an orange/cyan triangle in the upper right corner).

Minimum, maximum, and average response times are displayed at the bottom of each table. A response time is the amount of time between a Command and its Reply. Commands and Replies are tied together by looking for equal transaction numbers in the PCCC layer. Negative response times and response times that exceed 10 seconds are discarded (the former is an error and the latter is assumed to be an error). In the minimum and maximum fields, the Command and Reply frame numbers can be displayed by checking the “Show frame numbers” checkbox.

The device number is displayed in the header and in each corner of the dialog to enable easy identification of each dialog when multiple device dialogs overlap each other on the screen.

The top table of the Device Transactions dialog shows statistics for transactions which begin when the device specified in the dialog header receives Commands from a device specified at the top of a table column.

Row	Description
Recvd Cmds	Commands that the header device received from a column device.
Sent Cmd ACKs	ACKs that the header device sent to a column device in response to a Command from the column device.
Sent Cmd NAKs	NAKs that the header device sent to a column device in response to a Command from the column device.
Sent Replies	Replies that the header device sent to a column device.
Recvd Reply ACKs	ACKs that the header device received from a column device in response to a Reply from the header device.
Recvd Reply NAKs	NAKs that the header device received from a column device in response to a Reply from the header device.
Min Response Time	Minimum response time
Max Response Time	Maximum response time
Avg Response Time	Average response time
No Reply Within 60 Secs	Number of occurrences of no reply within 60 seconds

The bottom table of the Device Transactions dialog shows statistics for transactions which begin when the device specified in the dialog header sends Commands to a device specified at the top of a table column.

Row	Description
Sent Cmds	Commands that the header device sent to a column device.
Recvd Cmd ACKs	ACKs that the header device received from a column device in response to a Command from the header device.

Recvd Cmd NAKs	NAKs that the header device received from a column device in response to a Command from the header device.
Recvd Replies	Replies that the header device received from a column device.
Sent Reply ACKs	ACKs that the header device sent to a column device in response to a Reply from the column device.
Sent Reply NAKs	NAKs that the header device sent to a column device in response to a Reply from the column device.
Min Response Time	Minimum response time
Max Response Time	Maximum response time
Avg Response Time	Average response time
No Reply Within 60 Secs	Number of occurrences of no reply within 60 seconds

The drop down menu provides selections to display the data as:

- Message Count
- Message Count Percentage (Percentage of the total number of messages)
- *Byte Count*
- Byte Count Percentage (Percentage of the total number of bytes)

Clicking the *Apply settings to all transaction dialogs* button applies the selection in the drop down box to the *Transaction Summary* dialog.

10.8.3.2 Device Token Rotations Dialog

The Device Token Rotation dialog is accessed by clicking on the Rotations button in a Device Transactions dialog. The Device Token Rotation dialog displays minimum, maximum, average, and total values for the selected *device* against the following parameters:

- duration token held
- total Bytes sent per token rotation (this is all bytes from all messages)

- *Command* Bytes Sent Per Token Rotation
- *Reply* Bytes Sent Per Token Rotation

For the minimum and maximum values, the Date and Time of Occurrence and the Frame range are also displayed against each of the above parameters. The frame range begins with the frame in which the specified device receives the token, and ends with the frame in which the specified device sends the token to another device. This means that the last frame of a given token rotation and the first frame of the next token rotation are the same frame. The device number is displayed in the header and in each corner of the dialog to enable easy identification of each dialog when multiple device dialogs overlap each other on the screen. Pressing the Transactions button returns to the Device Transactions dialog.

NOTE:

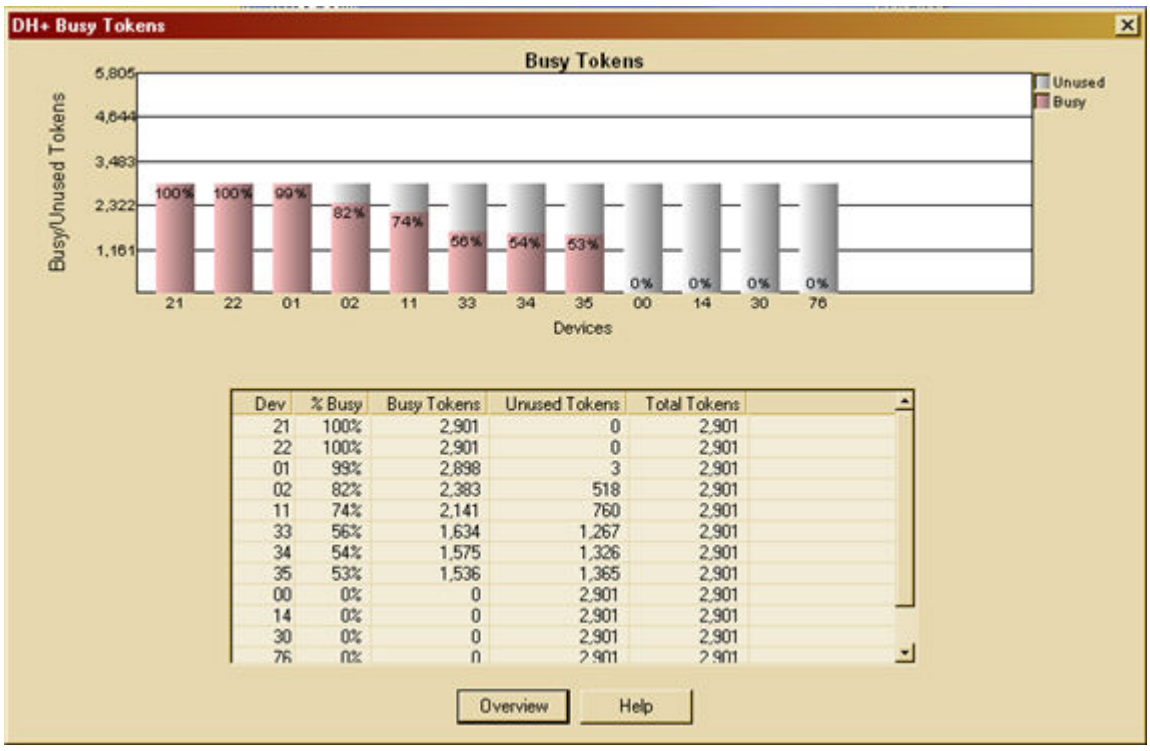
The Duration Token Held field is negative (and is discarded) when the same device receives the token, then sends it, then receives it again within what appears to be a single token rotation (when this happens it is typically due to missing frames). Since DH+ Stats simply saves the time-stamp each time and subtracts the receive time-stamp from the send time-stamp, the result is negative (and is discarded).

10.8.4 Network Statistics

10.8.4.1 Busy Tokens Dialog

To access the Busy Tokens dialog, select *Busy Tokens* from the *View* menu in the Overview dialog.

The Busy Tokens dialog shows busy *token* data in both a graph and a table.



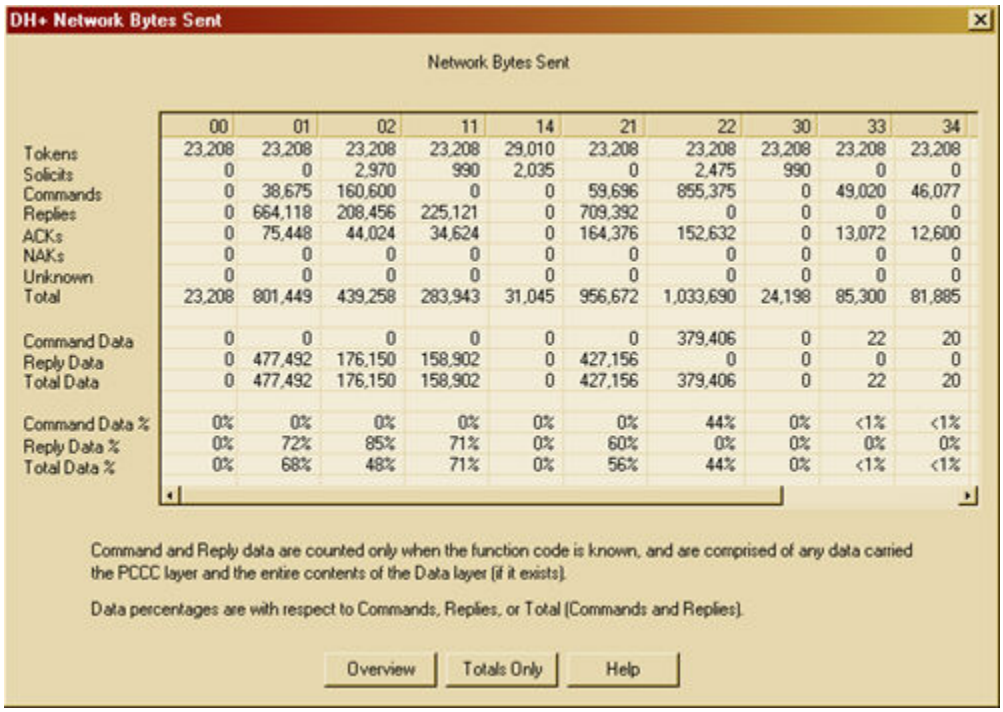
The **graph** displays the percentage of busy and unused tokens for the active devices in stacked bars, mauve for Busy, white for Unused.

The **table** displays:

- Device Identifier
- Percentage of busy tokens
- Number of busy tokens
- Number of unused tokens
- Total tokens

10.8.4.2 Network Bytes Sent Dialog

To access the Network Bytes Sent dialog, select *Network Bytes Sent* from the *View* menu or select the Network button from the Overview dialog.


DH+ Network Bytes Sent
Network Bytes Sent
Command and Reply data are counted only when the function code is known, and are comprised of any data carried the PCCC layer and the entire contents of the Data layer (if it exists).
Data percentages are with respect to Commands, Replies, or Total (Commands and Replies).
Overview
Totals Only
Help

	00	01	02	11	14	21	22	30	33	34
Tokens	23,208	23,208	23,208	23,208	29,010	23,208	23,208	23,208	23,208	23,208
Solicits	0	0	2,970	990	2,035	0	2,475	990	0	0
Commands	0	38,675	160,600	0	0	59,696	855,375	0	49,020	46,077
Replies	0	664,118	208,456	225,121	0	709,392	0	0	0	0
ACKs	0	75,448	44,024	34,624	0	164,376	152,632	0	13,072	12,600
NAKs	0	0	0	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0	0	0	0
Total	23,208	801,449	439,258	283,943	31,045	956,672	1,033,690	24,198	85,300	81,885
Command Data	0	0	0	0	0	0	379,406	0	22	20
Reply Data	0	477,492	176,150	158,902	0	427,156	0	0	0	0
Total Data	0	477,492	176,150	158,902	0	427,156	379,406	0	22	20
Command Data %	0%	0%	0%	0%	0%	0%	44%	0%	<1%	<1%
Reply Data %	0%	72%	85%	71%	0%	60%	0%	0%	0%	0%
Total Data %	0%	68%	48%	71%	0%	56%	44%	0%	<1%	<1%

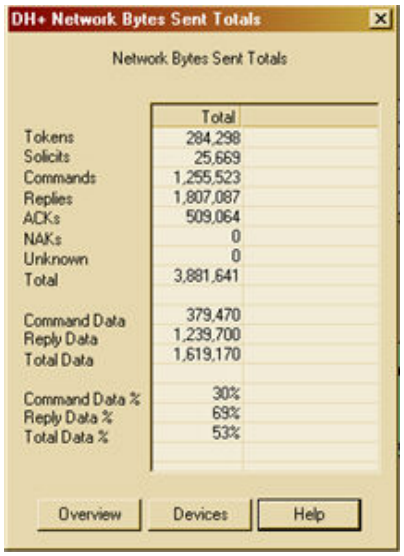
The Network Bytes Sent dialog is simple and comprehensive. It shows the number of bytes sent by each *device*, by message type, including unknown messages. The value in the Total column of the Total row is the same number displayed in the *Byte Count* field of the Overview dialog.

The device numbers are displayed at the top of each column.

The **Totals Only** button displays the Network Bytes Sent Totals dialog.

10.8.4.3 Network Bytes Sent Totals Dialog

To access the Network Bytes Sent Totals dialog, select *Network Bytes Sent Totals* from the *View* menu in the Overview dialog, or click on the *Totals Only* button on the *Network Bytes Sent* dialog.



The Network Bytes Sent Totals dialog is a copy of the Totals column of the Network Bytes Sent dialog. The Devices button displays the Network Bytes Sent dialog.

DH+ Statistics uses the size of the frame as it appears on the DH+ wire to compute Byte Count. This is equivalent to the size of the FTS physical frame minus one byte.

10.8.4.4 Network Event Log Dialog

To access the Network Event Log dialog, click on the *Log* button or select *Network Event Log* from the *View* menu in the Overview dialog.

The Network Event Log dialog displays a breakdown of various network events that are automatically logged. This information provides additional details about the health of the network. This log stores the most recent 2000 events. Checkbox selections at the bottom of the dialog determine which events the system logs.

10.8.4.5 Events

The system logs the following events:

Event	Description	Color and Shape in Grid
Appeared	*Device* appeared for the first time	Green square

Dropped off bus	Device dropped off the bus	Red square
Reappeared	Device reappeared after dropping off the bus	Blue square (supercedes a yellow square)
Sent *NAK* to a *Command* or *Reply*	Device sent a NAK immediately after receiving a Command or Reply	Yellow square
Had error in decode or summary panes of Frame Display	Device had one or more decode errors.	Yellow square
Token/*Solicit*/Command/Reply sent but not by token holder	Device sent a token, solicit, Command, or Reply but was not the most recent device to be sent the token.	Yellow square
Sent *ACK* or NAK but hadn't received Command or Reply	Device sent an ACK or NAK, but the previous message on the wire was not a Command or Reply that was sent to that device.	Yellow square
Sent to an invalid (out of range) device number	Device sent a message with a destination device number that was not in the range 00..77 octal.	Yellow square
Sent from an invalid (out of range) device number	A source device number in a message was not in the range 00..77 octal.	n/a
Sent to itself	The source and destination device numbers in a message were the same.	Yellow square
Long Responder - (reply took longer than 5 seconds)	Device was the destination of a Command and immediately sent ACK but the reply took between 5 and 60 seconds	Cyan triangle in upper-right-corner of square

Non-Responder - (no reply within 60 seconds)	A non-responder takes more than 60 seconds to respond or does not respond at all	Orange triangle in upper-right-corner of square
Non-Responder - (no ACK or NAK)	Device was the destination of a Command and didn't send an ACK or NAK	Yellow square
Gap in frame sequence numbers	One or more frames are missing as determined by noting a gap in the frame sequence numbers. Detailed info is shown in the "Missing and Excluded Frames" dialog.	n/a
Duration between frames exceeds 0.5 seconds	Bytes are assumed to be missing because the duration between two adjacent frames exceeded 0.5 seconds. Detailed info is shown in the "Missing and Excluded Frames" dialog.	n/a

10.8.4.6 Table Columns

- Each table column is sorted in each direction by clicking on the column header.
- When any column except the first (Seq) is sorted, the first column is used as a secondary sort key so that the seq nums are also sorted within each range of equal fields in the sorted column.
- When writing to the CSV file, the current sort order is used.
- While a device is absent, Non-Responder events for that device are condensed (logged only once with a count range, with all other fields set to the first event in the range).
- All future occurrences of an event are logged if the corresponding event checkbox is checked, and excluded if the corresponding event checkbox is unchecked.
- Sequence number gaps indicate excluded or condensed events.

Table columns are as follows:

Column	Description
Seq	Event sequence number, starting at 1. Every event receives a sequence number, even events that are not logged (due to being excluded or condensed).
Dev	Device number
Event	Event description
Count	Number of occurrences of that combination of Event, Dev, and Msg Dev (device numbers that appear in the Event field are ignored). This is shown as a range for condensed events.
Frame	Frame number where event occurred.
Rotation	Token rotation number where event occurred. In the case of a gap in the frame sequence numbers or more than 0.5 seconds between frames, the token rotation is excluded and its number is shown in parentheses. Note that the next included token rotation has the same number (i.e. excluding a token rotation does not result in a gap in the token rotation numbers).
Timestamp	Time of occurrence
Msg Dev	Number of device that sent a Command or Reply. Set only when the event is "Non-Responder...".
Msg Frame	Frame number of a Command or Reply. Set only when the event is "Non-Responder ...".

10.8.4.7 Top Talkers Dialog

The *Top Talkers* dialog displays statistics on bandwidth usage by *device*.

You access the Top Talkers dialog by clicking on the More button located above the Top Talkers table on the Overview dialog, or by selecting Top Talkers from the View menu on the Overview dialog.

The graph displays *Command* and *Reply* byte count sent by a single device in byte count order. All devices that have ever been present on the bus appear in the graph, regardless of whether they sent any Command or Reply messages. Graph bars display the byte count percentage at the top of each bar.

The table displays device Command and Reply byte count, percentage of total Command and Reply bytes on the network, Command and Reply message count, percentage of total Command Reply message count, and average length. The table sorts the device list by Byte

Count , allowing the user to identify which devices use most of the available network bandwidth.

The calculated statistics displayed in the Top Talkers table and graph only includes data from Command and Reply messages, and does not include data from required network Protocol messages (*ACK*, *NAK*, *Token* and *Solicit*).

Top Talkers Column Headings:

- Dev Num – Device address in octal
- Byte Count* – Number of Command and Reply bytes sent by a device
- %Bytes – Percentage of all network Command and Reply bytes sent by a device
- Msg Count – Number of Command and Reply messages sent by a device
- %Msgs – Percentage of all network Command and Reply messages sent by a device
- Avg Len – Average Length of Command and Reply messages sent by a device

* DH+ Statistics uses the size of the frame as it appears on the DH+ wire to compute Byte Count. This is equivalent to the size of the FTS physical frame minus one byte.

10.8.4.8 Top Conversations Dialog

The *Top Conversations* dialog displays conversation statistics.

Access the Top Conversations dialog by clicking on the More button located above the Top Conversations table on the Overview dialog, or by selecting *Top Conversations* from the *View* menu on the *Overview* dialog.

A "conversation" consists of *Command* and *Reply* messages sent between two specific devices. The graph shows command and reply *byte count* for each pair of devices sorted first by byte count and then by device pair. All device pairs are shown for all devices that appeared on the bus, regardless of whether the devices in the pair communicated with each other.

The scale across the bottom of the graph identifies the device pair using their two digit octal number identifiers, and the scale up the side of the graph lists the byte count. Each bar provides a graphic representation of its associated device pair's byte count usage with respect to other device pairs on the network, and the percentage of total byte usage by each device pair appears on each bar.

The table below the graph sorts the device list by Byte Count. The statistics displayed in the table includes only data from device-controlled command and reply messages, and does not include data from required protocol messages (*ACK*, *NAK*, *Token* and *Solicit*).

Top Conversations Column Headings include:

- Dev Num – Device pair addresses in octal
- Byte Count* – Number of Command and Reply bytes sent between a device pair

- %Bytes – Percentage of all network Command and Reply bytes sent between a device pair
- Msg Count – Number of Command and Reply messages sent between a device pair
- %Msgs – Percentage of all network Command and Reply messages sent between a device pair
- Avg Len – Average Length of Command and Reply messages sent between a device pair

* DH+ Statistics uses the size of the frame as it appears on the DH+ wire to compute Byte Count. This is equivalent to the size of the FTS physical frame minus one byte.

10.8.4.9 Token Rotations Dialog

You access the Token Rotations dialog by clicking on the More button located above the Token Rotations table on the Overview dialog, or by selecting Token Rotations from the View menu on the Overview dialog.

The Token Rotations dialog displays the values of the last 2000 maximum and the last 2000 minimum Token Rotation Times, and is limited to 4000 total entries. If no more than 4000 token rotations are processed, then all are shown.

The table shows a sequence number (where the first token rotation is number 1), the *token rotation*, duration, the date and time of occurrence, and the number of the first frame in the token rotation. The graph shows token rotation durations in order of occurrence. These values identify the best and worst case Token Rotation Times. Token Rotation Times directly affect the throughput capabilities of the network.

Sorting

The table can be sorted by sequence number or token rotation duration in ascending or descending order. Whenever the sorting method is changed, the table automatically scrolls back to the top. Choose the sorting method from the drop down field just above the table display. The graph, however, cannot be sorted.

Scrolling

When the table or graph scroll bar slider is at the top or leftmost it stays there while additional events accumulate in the log, otherwise it is adjusted as necessary so that the first displayed entry retains its position. If that entry is removed (because it is no longer one of the 2000 max or 2000 min durations), then an adjacent entry takes its place on the display.

Graph Points

The number of points in the graph is selectable in multiples of 10 from 10 to 300. Click the up and down arrows in the *Max Points* field to change the number of points displayed in the graph.

Selecting Entries

Selecting an entry in the graph automatically selects the corresponding entry in the table and vice versa , regardless of how the data is sorted in the table. Use the *Ctrl* and *Shift* keys to select contiguous and non-contiguous entries. When a graph entry is selected and the corresponding entry is not already visible in the table, the selected entry is highlighted and scrolled to the top of the table. When a table entry is selected and the corresponding entry is not already visible in the graph, the selected entry is highlighted and scrolled to the middle of the graph.

Y-Axis Max

The "Y-Axis Max" field sets the height of the y-axis and is provided primarily to allow the user to deal with the degenerate case of the entire network pausing for a long time. When that happens, the single token rotation duration that includes the time that the network was paused can dwarf the other token rotation durations to the point of near-invisibility. Setting the y-axis height to an appropriate value pushes the outlier(s) past the top of the graph while placing the rest of the values below the top of the graph. Checking the Auto box causes the y-axis height to be adjusted dynamically such that the height of the largest token rotation duration is 95-99% of the height of the graph (regardless of whether that token rotation duration is currently visible on the graph). The Auto box is checked by default.

The **Token Rotations Summary** displays minimum, maximum, average, and current values against the following parameters:

- Duration (the token rotation duration time)
- Date and Time of Occurrence (of token rotation)
- Frame (the number of the first frame in the token rotation)
- Busy (the number of busy tokens)
- %Busy (the percentage of busy tokens)

The following parameters display "Message Count", or "*Byte Count*" depending upon the selection made in the *Messages* drop down box located just above the Token Rotations Summary table.

- *Token*
- *Solicits*
- *Commands*
- *Replies*
- *ACKs*
- *NAKs*

10.8.4.10 Transactions Summary Dialog

Access the Transactions Summary dialog by clicking the *Transactions* button on the Overview dialog or selecting *Transactions Summary* from the *View* menu on the *Overview*

dialog. This dialog lists a breakdown of the *Command* and *Reply* transactions as well as response times for each *device* on the network.

On a well-behaved network with no errors, the numbers of Commands, Command ACKs, Replies, and Reply ACKs are all equal. These numbers can be unequal in the table due to many factors, including transmission noise, partial *token rotations* discarded by DH+ Stats (this is normal behavior), un-captured frames (frames that occurred before or after the capture session), frames missed by DH+ Stats, and absent devices. To determine whether network or device errors have occurred, consult either the Network Event Log or the Active Devices grid (look for a device box that is yellow, red, or blue, or has a red triangle in the upper right corner).

Response time statistics reflect network throughput and assist with identifying worst-case conditions.

The top table of the Transactions Summary dialog shows statistics for transactions which begin when other devices receive Commands from a device specified at the top of a table column.

Row	Description
Recvd Cmds	Commands that other devices received from a column device.
Sent Cmd ACKs	ACKs that other devices sent to a column device in response to a Command from the column device.
Sent Cmd NAKs	NAKs that other devices sent to a column device in response to a Command from the column device.
Sent Replies	Replies that other devices sent to a column device.
Recvd Reply ACKs	ACKs that other devices received from a column device in response to a Reply from other devices.
Recvd Reply NAKs	NAKs that other devices received from a column device in response to a Reply from other devices.
Min Response Time	Minimum response time
Max Response Time	Maximum response time
Avg Response Time	Average response time
No Reply Within 60 Secs	Number of occurrences of no reply within 60 seconds

The bottom table of the Transactions Summary dialog shows statistics for transactions which begin when other devices send Commands to a device specified at the top of a table column.

Row	Description
Sent Cmds	Number of commands received
Recvd Cmd ACKs	ACKs that other devices received from a column device in response to a Command from the other device.
Recvd Cmd NAKs	NAKs that other devices received from a column device in response to a Command from the other device.
Recvd Replies	Replies that other devices received from a column device.
Sent Reply ACKs	ACKs that other devices sent to a column device in response to a Reply from the column device.
Sent Reply NAKs	NAKs that other devices sent to a column device in response to a Reply from the column device.
Min Response Time	Minimum response time
Max Response Time	Maximum response time
Avg Response Time	Average response time
No Reply Within 60 Secs	Number of occurrences of no reply within 60 seconds

Clicking the *Show Frame Numbers* check box adds the frame numbers to the Minimum Response Time and Maximum Response Time associated with this data in both tables.

The drop down menu provides selections to display the data as:

- Message Count
- Message Count Percentage (Percentage of the total number of messages)
- *Byte Count*
- Byte Count Percentage (Percentage of the total number of bytes)

Clicking the *Apply settings to all transaction dialogs* button applies the selection in the drop down box to the individual Device Transaction dialogs.

10.8.4.11 Top Listeners Dialog

Access the Top Listeners dialog by selecting *Top Listeners* from the *View* menu on the *Overview* dialog.

The graph displays *Command* and *Reply byte count* received by a single device in byte count order. All devices that have ever been present on the bus appear in the graph, regardless of whether they received any Command or Reply messages. Graph bars display the byte count percentage at the top of each bar.

The table displays device Command and Reply byte count, percentage of total Command and Reply bytes on the network, Command and Reply message count, percentage of total Command Reply message count, and average length. The table sorts the device list by Byte Count .

The calculated statistics displayed in the Top Listeners table and graph includes only data from Command and Reply messages, and does not include data from required network protocol messages (*ACK*, *NAK*, *Token* and *Solicit*).

Top Listeners Column Headings:

- Dev Num – Device address in octal
- Byte Count* – Number of Command and Reply bytes received by a device
- %Bytes – Percentage of all network Command and Reply bytes received by a device
- Msg Count – Number of Command and Reply messages received by a device
- %Msgs – Percentage of all network Command and Reply messages received by a device
- Avg Len – Average Length of Command and Reply messages received by a device

* DH+ Statistics uses the size of the frame as it appears on the DH+ wire to compute Byte Count. This is equivalent to the size of the FTS physical frame minus one byte.

10.8.5 DH+ Statistics Files

10.8.5.1 CSV Files

You can create a CSV file from the Statistics window.

1. Open the *File* menu on the Overview dialog
2. Selecting *Make CSV File*.

DHPlus Statistics creates an Excel spreadsheet file and displays the *Save As* dialog. The CSV file contains all of the tabulated information from all dialogs in DHPlus Statistics for the current file. The contents of tables that have a selector box are displayed separately for each possible entry in the selector box with the exception of the Token Rotations dialog where only Ascending Sequence and Descending Duration are displayed. Depending on the amount of statistical data generated, the Excel spreadsheet may contain tens of thousands of rows.

Note: This menu entry is not available while capturing live data, reading a capture file, or loading a statistics file.

10.8.5.2 Statistics Files

The statistics file contains all of the stats data in binary format. It has the base name of the capture file and the extension "sts", and is located in the same directory as the capture file. It is created automatically when a capture file is opened or when a live capture is begun, and is updated every 10 seconds while frames are being received and once more when frames stop being received. It's closed after each update so that it persists after a system crash.

When a capture file is opened, the associated stats file is loaded if it exists. Displaying a stats file results in the exact same stats data being displayed that were displayed when either the capture file was closed or live mode was exited, except that the Status field on the Overview dialog says "Stats file loaded" instead of "Done reading capture file".

Each stats file contains the version number of DH+ Stats that created it followed by the version number of the stats file itself.

A stats file that reflects only part of the capture file results when the capture file is closed before DH+ Stats has received all of its frames. When such a stats file is loaded, the Status field on the Overview dialog indicates what percentage of the capture file is reflected by the stats file.

Currently, DH+ Stats does not verify that the stats file was derived from the capture file. Because of this, it's possible for the capture file and stats file to get out of sync if one or the other is copied from somewhere else. In that case, the stats file can be recreated by selecting "Recreate Stats File" from the Overview dialog File menu.

When capturing to a buffer, the stats file is named "DhPlusStats-yyyy-mm-dd_HHMMSS.sts", where yyyy = year, mm = month, dd = day, HH = hours (00..23), MM = minutes, and SS = seconds (this is, incidentally, the same format used in FTS for capture to series). The only way to load such a stats file is to rename an arbitrary capture file to the same name as the stats file but with a "cfa" extension and open it. Clearly this is a very bad way to do it as it creates a bogus capture file and also defeats the FTS model of all screens pertaining to the open capture file, but it's all that's available until DH+ Stats API is augmented. It does, however, make it possible for a user to view a stats file that may have been many days or weeks in the creating. Capturing to a file is a far better approach since both the stats file and the capture file are created.

When a wrapping capture is performed, FTS stops sending frames to DH+ Stats as soon as the next frame for DH+ Stats is overwritten by the frame compiler. At some point this probably changes so that FTS instead sends the most recent frame, but even then large numbers of frames is not seen by DH+ Stats.

10.8.5.3 Backward Compatibility

All statistics files from later versions are backward compatible. Statistics files produced by earlier versions can be read by any subsequent versions. If DH+ Stats has a version number later than the statistics file, the system displays a screen that lists the differences.

11 Transmitting Data

11.1 Transmit Window

To open this window:

Click the Transmit icon  on the Control window. If the Transmit icon is not active, open the I/O Settings window  and set the Operating Mode to Source.

The Transmit window is used to tell the analyzer what string or file you want to transmit, and start and stop data transmission.

11.2 Transmitting Strings

To access this feature:

Click the Transmit icon  on the Control window. If the Transmit icon is grayed out, you have to go to the I/O Settings window  and choose Source for your operating mode. On the Transmit window, click the String tab.

1. Type the string you want to send in the large text box. The analyzer interprets your string on the basis of which character set is currently active. Click on the History button  to the right of the string window to choose a previously used string.
2. Click the Transmit Once radio button to indicate that the string should be sent once. Choose Transmit Continuously to send the string continuously. Click Times to Transmit and enter a number in the box to specify how many times to send the string.
3. Click on the Start Capture  icon.
4. Click on the Begin Transmitting icon  to transmit your string. The Begin Transmitting icon is grayed out while the string is being transmitted, and become active once transmitting is finished. If you chose to transmit once or multiple times, the analyzer sends your string and then stops transmitting. If you chose to transmit continuously, the analyzer sends the string until you click on the Pause Transmitting icon  or the Stop Transmitting icon  . Pause Transmitting and Stop Transmitting pause and stop transmission only; they have no effect on data capture.

11.3 Transmitting Files

To access this feature:

Click the Transmit icon  on the Control window. If the Transmit icon is grayed out, you need to go to the I/O Settings window  and choose Source for your operating mode. On the Transmit window, click the File tab.

The analyzer transmits files as is. For example, if you transmit a text file, the analyzer sends the text characters, but also sends any formatting instructions such as carriage returns, tab characters, etc., as their hex equivalents.

The analyzer capture files must first be exported to binary format before being transmitted. The analyzer capture files are in a special format, and if you transmit a the analyzer capture file in its native format, what you see bears no resemblance to the data you want to transmit. See Transmitting FTS Capture Files for more information.

1. Type in the name of the file you want to send in the File to Transmit box, or click the Browse button to locate your file.
2. Click on the appropriate radio button to choose how many times you want to transmit your file. You can transmit once, transmit multiple times, or send the file continuously. If you choose to transmit multiple times, type in the number of times you want to send the file in the box to the right of the Times to Transmit line.
3. Click on the Start Capture  icon .
4. Click on the Begin Transmitting  icon to transmit your file. The Begin Transmitting icon grays out while the file is being transmitted, and become active once transmitting is finished. If you chose to transmit once or multiple times, the analyzer sends your file and then stop transmitting. If you chose to transmit continuously, the analyzer sends the file until you click on the Pause Transmitting icon  or the Stop Transmitting icon  . Pause Transmit Transmitting and Stop Transmitting affect transmission only; they have no effect on data capture.

If you want to transmit the data in a the analyzer capture file, you need to convert the file to a generic format using the Export function. If you transmit a the analyzer capture file without converting it first, the analyzer sends the data, but it also sends all the other information stored in the capture file, such as timestamping information. See Transmitting FTS Capture Files for more information.

11.4 Transmitting FTS Capture Files

To transmit the data in a FTS capture file, you first need to export it to a binary format.

1. Open the capture file containing the data you want to transmit.
2. On the Control window, choose Export Events from the File menu.

3. Choose Binary Output.
4. In the Available Fields box, choose Char/Event Name. Click the Move One Item Right button (looks like ">") to add it to the Displayed Fields box. Remove any other fields in the Displayed Fields box.
5. Choose a filename in the Export box. The default file name is the name of your capture file, followed by the word "Events" (to distinguish it from a Frame export), with a .bin extension.
6. By default the file is saved in the same directory as the original capture file. Click on the Browse button to save your file to another location.
7. If you want to transmit just DTE data or DCE data, be sure to filter out the side you do not want. Also, you probably want to filter out Special Events.
8. Click Export.
9. The result is a .bin file, which you can transmit from the File tab of the Transmit window.

11.5 The Transmit Toolbar



Home - brings the Control window to the front.



I/O Settings - Opens the I/O Settings dialog.



Start Capture - Begins data capture to a single file or a series of files.



Close Capture File - Closes a capture file and stops data capture. Data can be reviewed and saved, but no new data is captured.



Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.



Clear- Discards the temporary file and clears the display.



Enter Sync Hunt - Used to resync when monitoring a bisync or monosync circuit. Sometimes when synchronization is lost, there is no indication to the analyzer that it needs to resync. Enter Sync Hunt causes the analyzer to start looking for sync characters and resynchronize.



Send - Tells the analyzer to begin transmitting.



Pause Transmitter - Pauses transmission. While transmitting is paused, the analyzer does not send data but it continues to capture data coming from the other device.



Stop Transmitting - Stops data transmission. The analyzer continues to capture data.

11.6String Formats

Note that any of the formats below can be combined. It is legal to transmit the ASCII string ABC$65$30, for example.

Entering Normal Text Characters

The system sends your string in whatever character set you are currently using. To change the character set, go to the Data menu in the Control Window, and choose a character set.

Examples:

To send the string "qwerty", you would type qwerty.

To send the string "hello, world", you would type hello, world.

Entering Characters in Hex

To transmit in hex, type a $ in front of your two digit byte. The $ symbol tells the analyzer that you are sending in hex. If you want to send more than one hex byte, you have to type the $ symbol in front of each byte.

You must have a two digit hex number after the $ for the analyzer to interpret the bytes as hex properly. Otherwise, the analyzer interprets the characters as if they belonged to a character set. For example, if you want to send an ASCII NUL, which is hex 00, and you type $0, the analyzer sends hex 24 followed by hex 30. The $ symbol is hex 24 in ASCII, and zero is hex 30. To send a hex 00, you must type $00.

Example:

To send hex 31 00 97, you would type $31$00$97.

Entering Control Characters

The ^ symbol is used to specify that what follows is a control character. You can transmit the control characters Ctrl-A through Ctrl-Z, and Ctrl-@, Ctrl-[, Ctrl-\, Ctrl-], and Ctrl--. For example, ^A sends Ctrl-A ($01) and ^@ sends ASCII NUL ($00).

The Escape Character

The \ is the escape character. It is used when transmitting special characters, in order to specify that the next character should be taken literally. These special characters are: $^&*()\. For example, to put an * in a string, enter *. To transmit a \, enter \\.

Specifying a Range of Characters

You can also send a range of characters by placing two periods between your first and last characters. For example, A..I generates the string ABCDEFGHI. It is important to note that A..I in ASCII is very different from A..I in EBCDIC. In ASCII, A..I is equivalent to $41..$49, while in EBCDIC A..I is equivalent to $C1..$C9. It is also legal to specify a descending range. For example, I..A generates IHGFEDCBA.

Sub-expressions

Sub-expressions are enclosed in (). The parentheses are not part of the sub-expression and are not transmitted. For example, (ABC) yields ABC. Sub-expressions are useful because you can specify a repeat count for them using the *. For example (ABC)*3 yields ABCABCABC.

Entering Baudot Characters

Since Baudot is only 5 bits it includes two shift characters. Shift In ($1F) means interpret all following characters as letters; Shift Out ($1B) means interpret all following characters as figures (punctuation, numbers, control codes, etc). When the analyzer is activated it assumes the letters mode. The shift characters are captured in the buffer just as other bytes. In source mode the analyzer automatically supplies the shift characters to the string you enter. For example, if you are in letter mode and enter the string 12AB, the analyzer sends $1B (Shift Out), $17 (1), $13 (2), $1F (Shift In), $03 (A), $19 (B).

NOTE: When you use hex notation to input a Baudot string, the analyzer does not insert shift characters.

More Examples

Enter	To Generate
\\\$\^\(\)*	\$^()*
\$.ABC.	$.ABC.
(ABC)*3\9	ABCABCABC9
($6b..$68)*2	kjihkjih
(A(BC)*2)*3	ABCBCABCBCABCBC
Aa..iZ	AabcdefghiZ

11.7 Flow Control when Transmitting

Flow Control is enabled in the I/O Settings window  . When flow control is active, the analyzer waits for a specified condition before sending data. This feature is typically used for testing printers, stat muxes, and other devices which must throttle the data flowing to them. The analyzer has a flow control status line at the bottom of the transmit window which tells you when flow control is active or inactive.

The analyzer supports both software and *hardware flow control*. *Software flow control* uses the Xon and Xoff values specified in the I/O Settings window. This means that if the analyzer receives an Xoff character while in source mode it stops sending data until an Xon character is received. DC1 and DC3 (hex 11 and hex 13 respectively) are most often used for software flow control. If you need to use other characters, simply enter the hex values that you want to use in the flow control boxes on the I/O Settings screen.

The analyzer supports both RTS/CTS and DTR/DSR hardware flow control. Selecting RTS/CTS means that the analyzer uses the RTS/CTS control signals to control data transmission. When sourcing DTE, the analyzer automatically asserts RTS and send data when CTS is asserted. While CTS is not asserted, the analyzer does NOT send data. When the analyzer is finished sending data, it de-asserts RTS. In DCE mode the analyzer reverses the meaning of RTS and CTS, responding to RTS as the flow control indicator even though this is a non-standard use of the signal.

Selecting DTR/DSR tells the analyzer to use the DTR/DSR control signals for flow control. When sourcing DCE, the analyzer automatically asserts and de-assert DSR and responds to DTR. When sourcing DTE, the analyzer automatically asserts and de-assert DTR and respond to DSR.

11.8 Changing Control Signals

Next to the Transmit String or File box are boxes for changing control signal states. You are able to change control signals only for the device which you are emulating. For example, if you are a DTE source, you are only able to change RTS and DTR. If you are a DCE source, you are able to change CTS, DSR, CD and RI.

To change a control signal, click on the box. A check mark means that the signal is high, while an empty box means that the signal is low.

11.9 Delays and Max Burst Size

When the analyzer transmits data, it first puts the data to be sent in a transmit buffer, and then sends the data out the serial port. There is a limit on the amount of data that can fit into the transmit buffer at one time. The Max Burst Size option allows you to control how many bytes are put into the transmit buffer before the data is transmitted, while the Delays allow you to control the timing of data bursts.

Max Burst Size

Max Burst Size allows you to control how many bytes are put into the transmit buffer at a time.

Example: Assume that the transmit buffer can hold up to 1000 bytes. If the Max Burst Size is set to 1000, the analyzer would fill up the buffer with 1000 bytes and then send the 1000 bytes. However, if you want to send only 500 bytes at one time, you would set the Max Burst Size to 500. The analyzer would put only 500 bytes into the transmit buffer before sending them, even though the buffer could hold up to 1000 bytes.

String and File Delays

String Delay inserts a delay between each transmission of a string.

To set this type of delay

- Click on the radio button for String Delay.
- Type a value in the box to tell the analyzer how long to set the delay
- Click on the down arrow to choose a time increment of milliseconds, seconds or minutes. A delay of 0 (zero) means that the analyzer does insert a delay.

Timing under 2000/XP is often dealt with in increments of 10 milliseconds. This means that if you request a delay that is not a multiple of 10, the actual delay is rounded up to the nearest 10 milliseconds.

Example: A delay of 40 seconds causes the analyzer to transmit the string, wait 40 seconds, and transmit the string again. This pattern repeats until either the string has been transmitted the specified number of times, or the user chooses to stop transmitting.

File Delay works in exactly the same way as String Delay.

Burst Delay

Burst Delay inserts a delay between each transmission of the transmit buffer. Remember that the Max Burst Size option effectively sets the size of the transmit buffer. The analyzer fills the buffer with data up to the Max Burst Size, and send the data. If a Burst Delay is set, the analyzer pauses the length of the delay, before filling up the transmit buffer again and repeating the process.

To set the size of the burst

- Type how many bytes to send in the Max Burst Size box.
- Set the delay by typing in the length of the delay in the Burst Delay box
- Choose a time increment of Milliseconds, Seconds or Minutes from the pull-down menu.

Example: You want to send 1000 bytes, wait 2 minutes, and repeat the pattern. Type in 1000 in the Burst Size box, and set the delay to 2 minutes. The analyzer sends 1000 bytes, using as many repetitions of the string or file as necessary to achieve the correct number of bytes, wait 2 minutes and send the string again.

Example: You want to send a 1000 byte file continuously, and insert a five second delay between each transmission of the file. However, you also want to send the file in increments of 400 bytes each, with a ten second delay between each group of 400 bytes. To set this up, you would set your Max Burst Size to 400, your File Delay to five seconds, and your Burst Delay to ten seconds.

The analyzer would send 400 bytes, wait ten seconds, send 400 bytes, wait ten seconds, send 200 bytes, wait five seconds (because the end of the file has been reached), and repeat the process until transmission was paused or stopped.

11.10 Transmit Options

To open this window:

Click the Transmit icon  on the Control window toolbar. On the Transmit window, click the Options icon  .

The Transmit Priority determines how much of a priority the system places on transmitting data versus updating the screen. On slower PC's, so much processor time can be taken up transmitting data, especially at higher data rates, that the screen never updates, making it appear that the PC has locked up. The Transmit Priority slider bar determines how much time to take transmitting data. When the Transmit Priority is high, the analyzer ensures that data gets transmitted before it updates the user interface. If the Transmit Priority is low, the analyzer allows the user interface more time.

The length of your transmit string plays a role in the amount of throughput achieved. Longer strings are more efficient and results in higher throughputs than shorter strings.

11.11 Pause Transmit

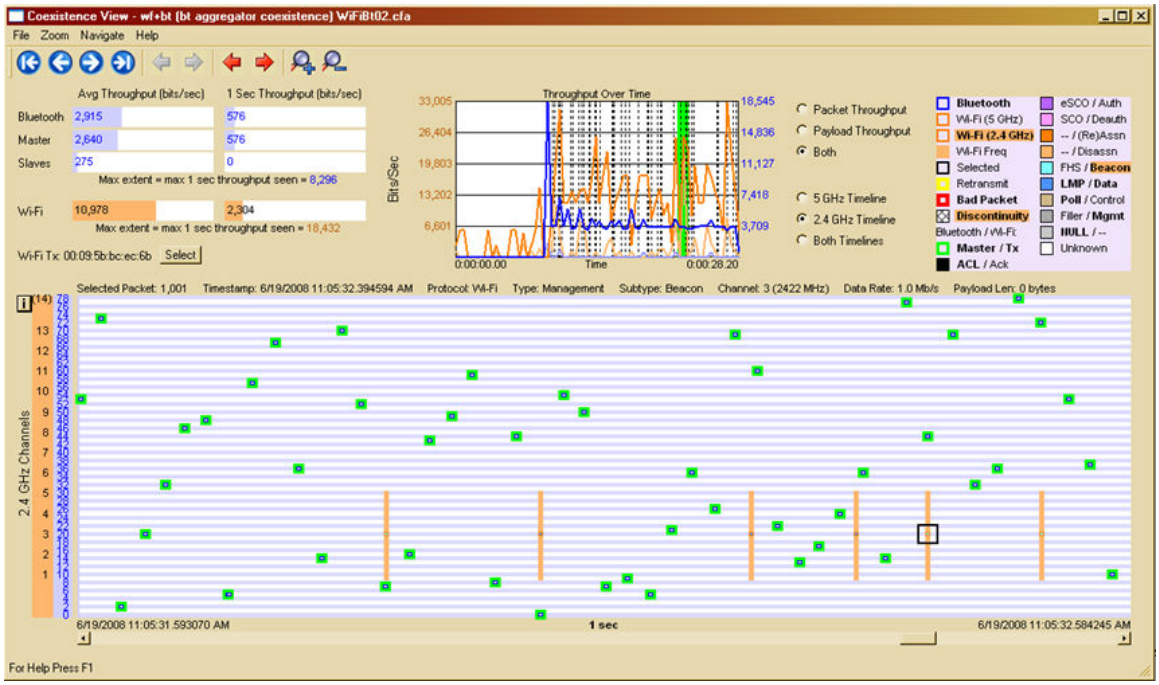
Pause Transmitting  temporarily halts data transmission. When transmission is resumed, the analyzer continues to send the rest of the data.

Stop Transmitting  halts transmission completely and any unsent bytes are thrown away. For example, if you are sending the ASCII string ABCD, and you paused transmission after AB had been sent, the analyzer remembers that it needed to send the CD. When transmission is resumed, the analyzer sends the CD. However, if you stop transmission after the AB has been sent, the analyzer throws away the CD. If you start transmission again with the same string, the analyzer transmits the string from the beginning.

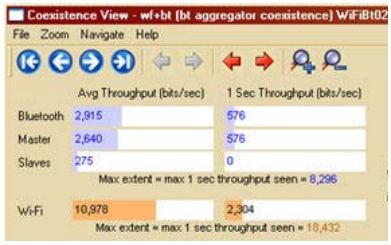
12 Coexistence View

12.1 Coexistence View Introduction

The Coexistence View displays both the Bluetooth® and the Wi-Fi channels frequencies in one view. You access the Coexistence View by selecting the icon from the Control Window, Frame Display, and Protocol Navigator toolbars or from the View menus.



12.1.1 Average Throughput/1 Second Throughput


Coexistence View - wf+bt (bt aggregator coexistence) WiFiBt02
File Zoom Navigate Help
Avg Throughput (bits/sec)
1 Sec Throughput (bits/sec)
Bluetooth 2,915 576
Master 2,640 576
Slaves 275 0
Max extent = max 1 sec throughput seen = 8,296
Wi-Fi 10,978 2,304
Max extent = max 1 sec throughput seen = 18,432

Bluetooth: Average Throughput/ 1 Second Throughput
This chart displays:

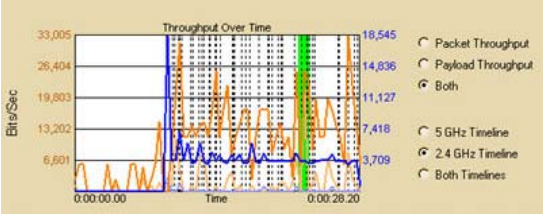
- Average Throughput in bits/seconds for all Bluetooth packets, Bluetooth Master packets, and Bluetooth Slave packets.
- One (1) Second Throughput in bits/seconds for all Bluetooth packets, Bluetooth Master packets, and Bluetooth Slave packets.

- Average Throughput = total packet/payload size divided by the duration of the entire session
- 1 second Throughput = packet/payload size during the most recent one second of the session

Wi-Fi: Average Throughput/ 1 Second Throughput
This chart displays the

- Average Throughput in bits/second and One (1) Second Throughput in bits/seconds for Wi-Fi.
  - Average Throughput = total packet/payload size divided by the duration of the entire session
  - 1 second Throughput = packet/payload size during the most recent one second of the session

12.1.2 Throughput Graph



The Throughput Graph displays throughput over time.

- Wi-Fi packet throughput is displayed as an orange line with corresponding orange numeric values on the left.
- Bluetooth packet throughput is displayed as a blue line with corresponding blue numeric values on the right.
- When you click anywhere in the graph, the timeline moves to the corresponding position in time.
- To keep the timeline and the throughput graph manageable, big jumps in packet timestamps are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the timestamp goes forward more than 2 seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph.
- You can show Packet Throughput, Payload Throughput, or both depending on which radio button to the right of the graph you select. The Avg Throughput and 1 Sec Throughput indicators are also affected.
- Payload Throughput is always less than Packet Throughput because a packet is never all payload.
- The green area in the throughput graph is called the viewport. Its position and width correspond to the beginning timestamp and duration of the timeline.

12.1.3 Legend



This legend identifies the color coding found in the timeline. When you select a packet in the timeline, its attributes are highlighted in the legend. A bold entry in the legend indicates that such a packet has been seen during the current session.

A Bluetooth packet has a blue outline, and a Wi-Fi packet has an orange outline.

12.1.4 Coexistence View Wi-Fi Tx Address



The Wi-Fi Tx Address displays a selected source address that you choose.



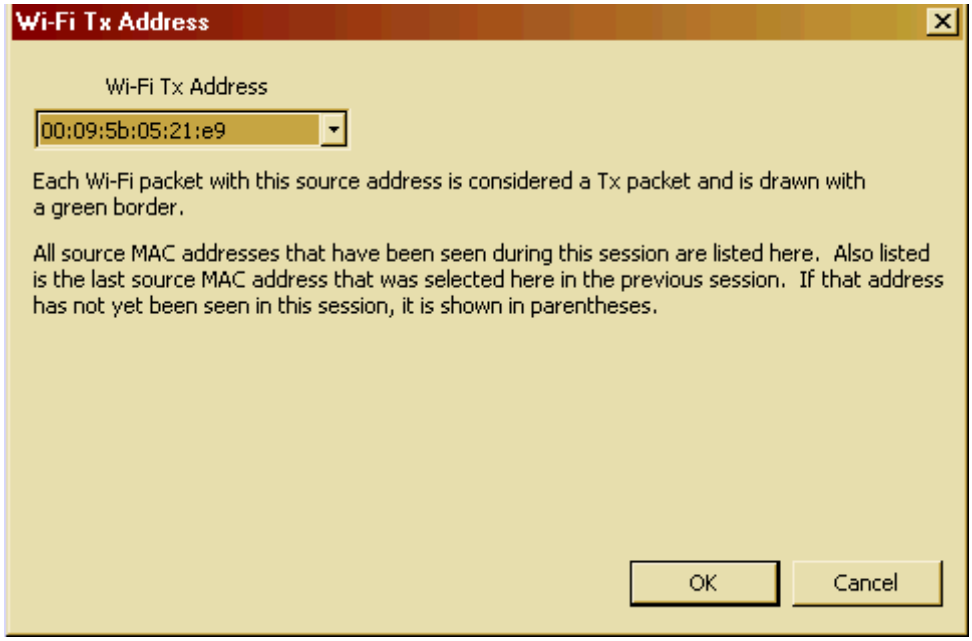
The specific address is highlighted with a green border.



To select a specific address:

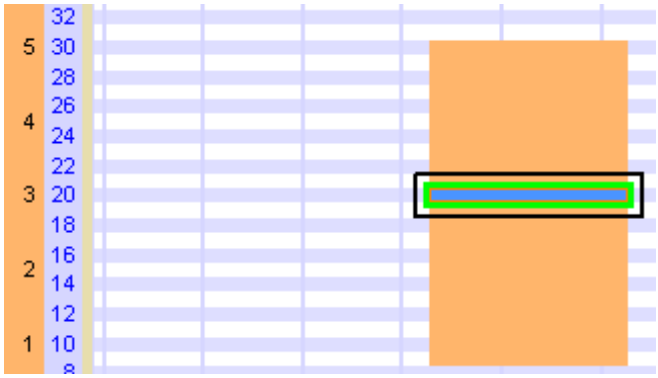
1. Click the **Select** button.

The Wi-Fi Tx Address dialog appears.


Wi-Fi Tx Address
Wi-Fi Tx Address
00:09:5b:05:21:e9
Each Wi-Fi packet with this source address is considered a Tx packet and is drawn with a green border.
All source MAC addresses that have been seen during this session are listed here. Also listed is the last source MAC address that was selected here in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.
OK
Cancel

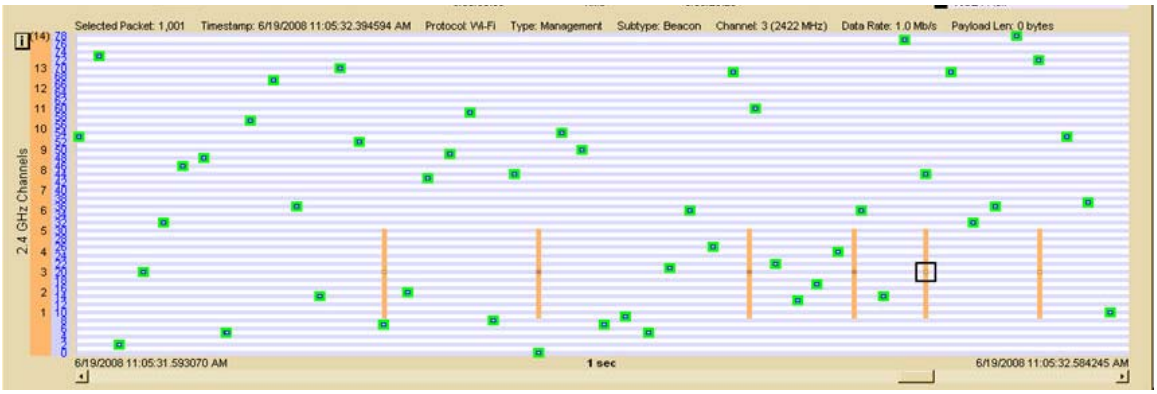
2. Select an address from the **drop-down list**.
3. Select **OK**.

The selected address appears with a green border around it.



4. Click on the links below to learn more about the specific *Bluetooth* and the Wi-Fi channel frequencies.

12.1.5 Timeline


Selected Packet: 1,001 Timestamp: 6/19/2008 11:05:32.394594 AM Protocol: Wi-Fi Type: Management Subtype: Beacon Channel: 3 (2422 MHz) Data Rate: 1.0 Mb/s Payload Len: 0 bytes
2.4 GHz Channels
6/19/2008 11:05:31.593070 AM
1 sec
6/19/2008 11:05:32.584245 AM

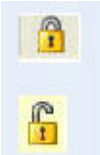
- The timeline shows Bluetooth and Wi-Fi packets within a specific period of time.
- The horizontal lines in the timeline are rows that correspond to Bluetooth and Wi-Fi frequencies.
- The vertical blue lines are Bluetooth slot markers for reference.
- The timeline displays Bluetooth and 2.4 GHz Wi-Fi packets together in the 2.4 GHz range when you select the 2.4 GHz Timeline radio button.
- The timeline displays 5 GHz Wi-Fi packets in the 5 GHz range when you select the 5 GHz Timeline radio button.
- The timeline displays Bluetooth/Wi-Fi packets in the 2.4 GHz range and Wi-Fi packets in the 5 GHz range when you select the Both Timelines radio button.
- The timeline duration is displayed underneath the timeline.
- Placing the mouse pointer on a packet in the timeline displays information about that packet in an information box.
- You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- On the 2.4 GHz Timeline, there are 79 Bluetooth and 14 Wi-Fi channels. Channel numbers are shown on the left side of the timeline. Bluetooth channel numbers have a blue background, and Wi-Fi channel numbers have an orange background.
- On the 5 GHz Timeline, there are 31 Wi-Fi channels. Channel numbers are shown on the left side of the timeline with an orange background. The channel spacing varies from 20 to 40 MHz.
- Each Bluetooth channel is 1 MHz wide with no channel overlap.
- Each Wi-Fi channel in the 2.4 GHz range is 22 MHz wide and overlaps. There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.The row labels for channels 1-13 are placed at the center frequency of each channel. Channel 14 is in parentheses because that channel's center frequency is above the top of the graph.Due to space limitations, each Wi-Fi channel in the 5 GHz

range is drawn with a fixed height instead of being sized and spaced relative to its width and distance from other channels.

- When both timelines are visible, selecting packets by dragging with the mouse applies to packets in both timelines, regardless of which timeline the mouse is in.
- Using the mouse scroll wheel scrolls horizontally in the chart. You can also use the arrow keys and the scroll bar at the bottom of the timeline to move within the timeline.
- Using the mouse scroll wheel + CTRL zooms. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Selecting the Information icons displays information about the Bluetooth and Wi-Fi channels.
- A green border appears around Wi-Fi Tx and Bluetooth Master.

12.2 Coexistence button bar

The button bar contains the following:



Lock - This locks the highlighted area in the display. Data will continued to be captured, but the highlighted area will move along the point where the lock was engaged.

Unlock - This unlocks the highlighted area so it will always remain at the right side of window where the newest data is displayed.

Note:The Lock/Unlock buttons only appears in live mode. Lock is automatically depressed when the user scrolls.



First Packet



Previous Packet



Next Packet



Last Packet



Previous Error Packet - This is active only when there is at least one qualifying packet to move back to. An error in Wi-Fi indicates a bad CRC. An error in Bluetooth indicates any error the data source can pass back.



Next Error Packet - This is active only when there is at least one qualifying packet to move forward to. An error in Wi-Fi indicates a bad CRC. An error in Bluetooth indicates any error the data source can pass back.



Zoom Tool - Click on the icon each time to zoom in from 4800 slots to 12 slots



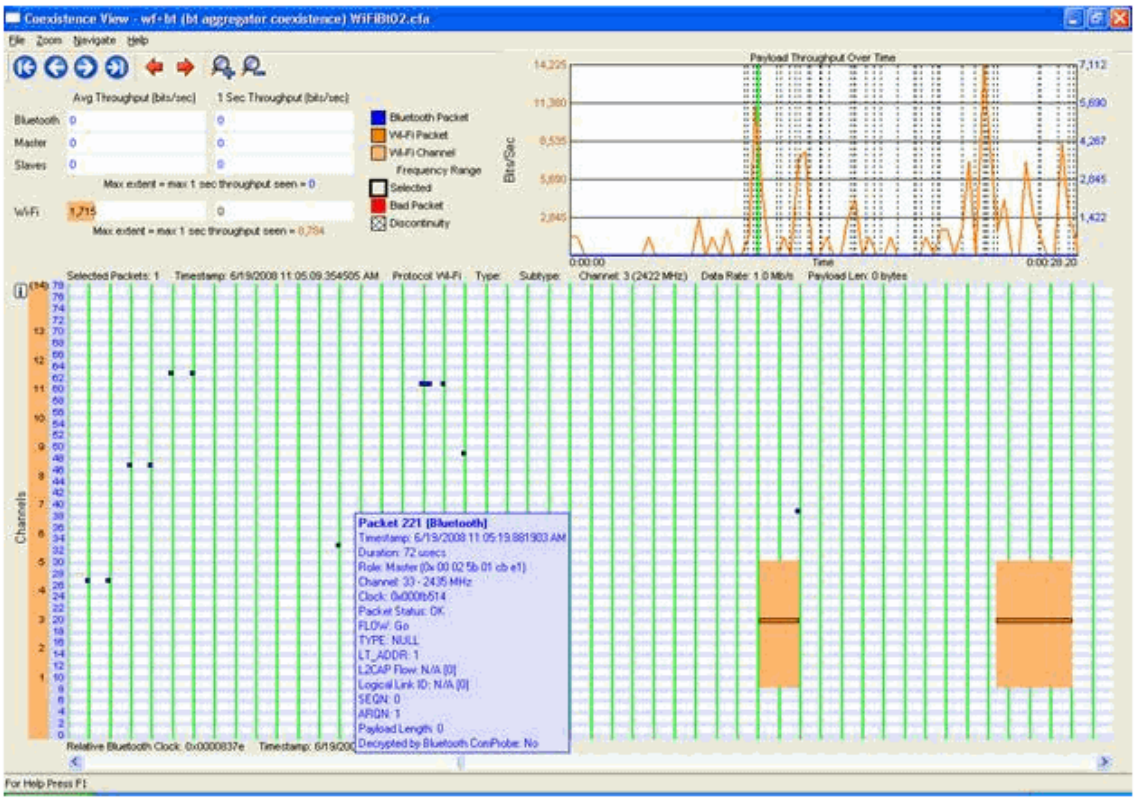
Zoom Tool - Click on the icon each time to zoom out from 12 slots to 4800 slots



Reset - This resets the live capture data.

12.3 Bluetooth® Channel Frequencies

There are 79 Bluetooth channels in the 2.4 GHz timeline. The Bluetooth channel numbers appear with a blue background along the left side of the timeline.



Each *Bluetooth* channel is 1 MHz wide with no channel overlap, unlike Wi-Fi channels which do overlap.

Selecting the icon displays channel information.

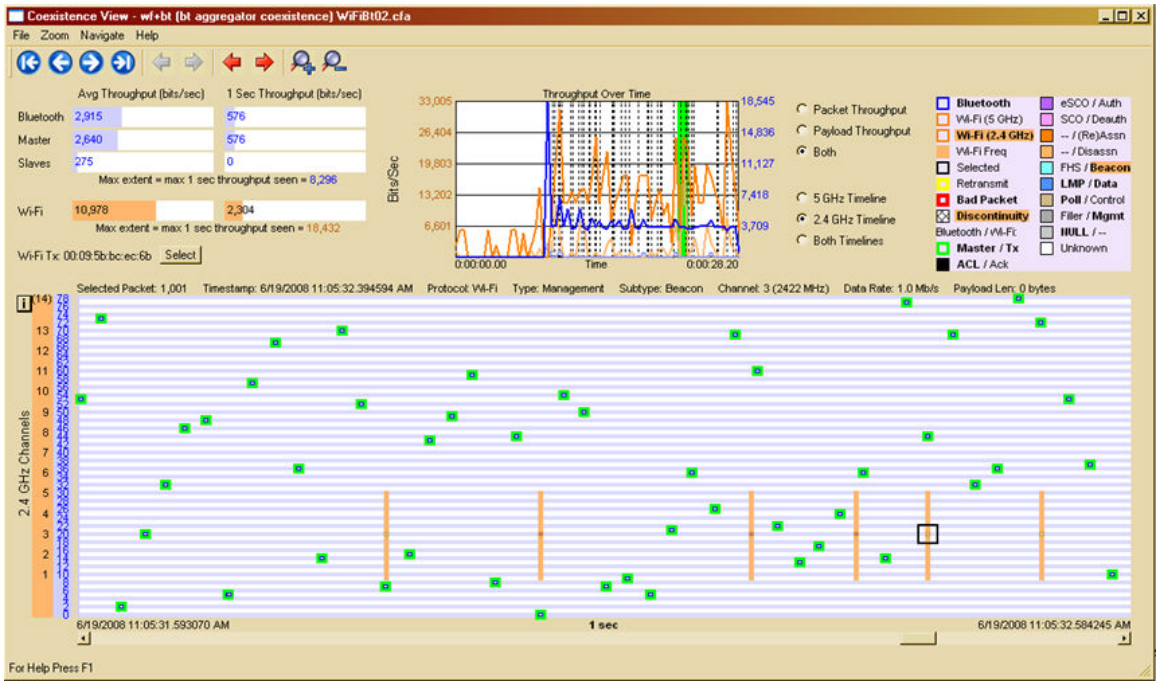
0=2402	12=2414	24=2426	36=2438	48=2450	60=2462	72=2474
1=2403	13=2415	25=2427	37=2439	49=2451	61=2463	73=2475
2=2404	14=2416	26=2428	38=2440	50=2452	62=2464	74=2476
3=2405	15=2417	27=2429	39=2441	51=2453	63=2465	75=2477
4=2406	16=2418	28=2430	40=2442	52=2454	64=2466	76=2478
5=2407	17=2419	29=2431	41=2443	53=2455	65=2467	77=2479
6=2408	18=2420	30=2432	42=2444	54=2456	66=2468	78=2480
7=2409	19=2421	31=2433	43=2445	55=2457	67=2469	
8=24010	20=2422	32=2434	44=2446	56=2458	68=2470	
9=24011	21=2423	33=2435	45=2447	57=2459	69=2471	
10=24012	22=2424	34=2436	46=2448	58=2460	70=2472	
11=24013	23=2425	35=2437	47=2449	59=2461	71=2473	

12.4 Wi-Fi Channel Frequencies - 2.4 GHz Channels

There are 14 Wi-Fi channels in the 2.4 GHz timeline. There are 11 channels available in the USA, 13 in Europe, and 14 in Japan.

The 14 Wi-Fi channels appear with an orange background along the left side of the timeline.

Selecting the icon displays channel information

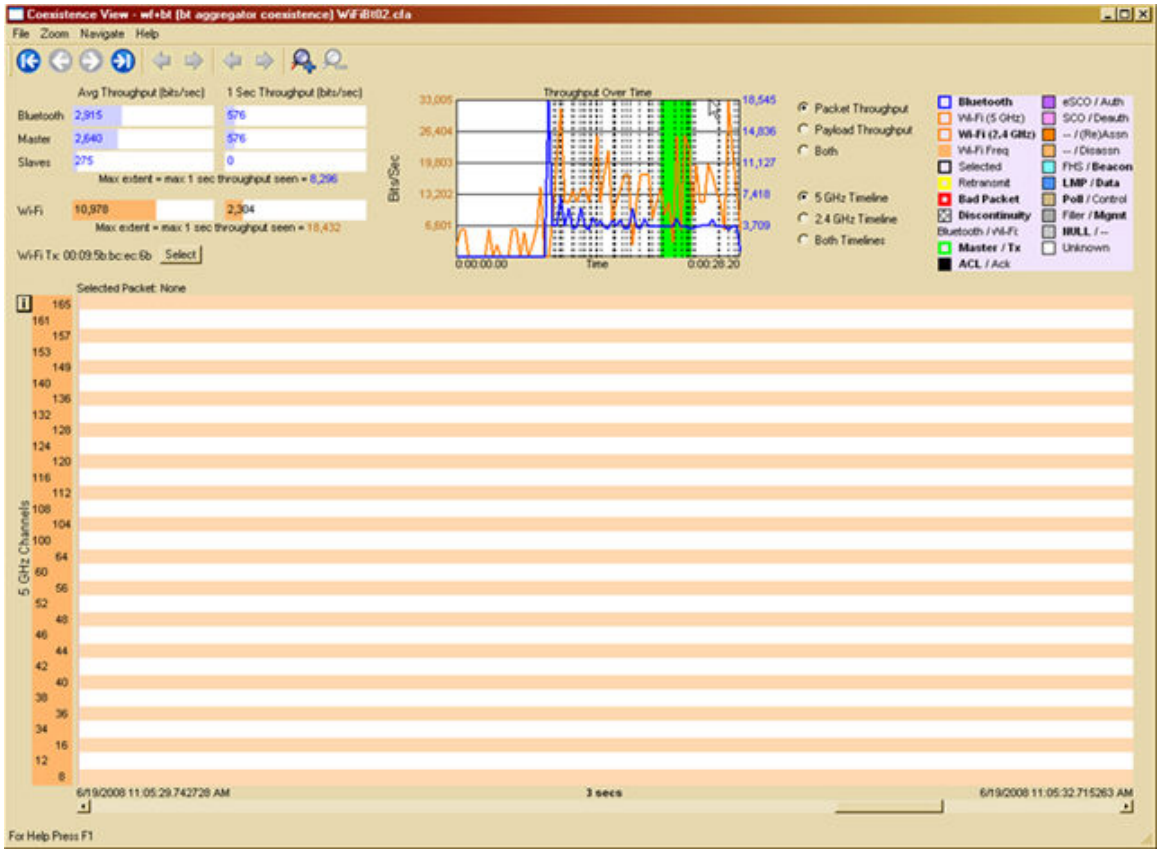


Each Wi-Fi channel is 22 MHz wide and overlap. There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.

1 = 2401-2423 MHz (centered at 2412 MHz) (USA, Europe, Japan)	8 = 2436-2458 MHz (centered at 2447 MHz) (USA, Europe, Japan)
2 = 2406-2428 MHz (centered at 2417 MHz) (USA, Europe, Japan)	9 = 2441-2463 MHz (centered at 2452 MHz) (USA, Europe, Japan)
3 = 2411-2433 MHz (centered at 2422 MHz) (USA, Europe, Japan)	10 = 2446-2468 MHz (centered at 2457 MHz) (USA, Europe, Japan)
4 = 2416-2438 MHz (centered at 2427 MHz) (USA, Europe, Japan)	11 = 2451-2473 MHz (centered at 2462 MHz) (USA, Europe, Japan)
5 = 2421-2443 MHz (centered at 2432 MHz) (USA, Europe, Japan)	12 = 2456-2478 MHz (centered at 2467 MHz) (Europe, Japan)
6 = 2426-2448 MHz (centered at 2437 MHz) (USA, Europe, Japan)	13 = 2461-2483 MHz (centered at 2472 MHz) (Europe, Japan)
7 = 2431-2453 MHz (centered at 2442 MHz) (USA, Europe, Japan)	14 = 2473-2495 MHz (centered at 2484 MHz) (Japan)
The row labels for Wi-FI channels 1-13 are placed at the center frequency of each channel	The row label for Wi-FI channel 14 is in parentheses because the channel's center frequency is above the top of the graph.

12.5 Wi-Fi Channel Frequencies - 5 GHz Channels

There are 165 Wi-Fi channels in the 5 GHz timeline. You access the 5 GHz Timeline by selecting the 5 GHz radio button.



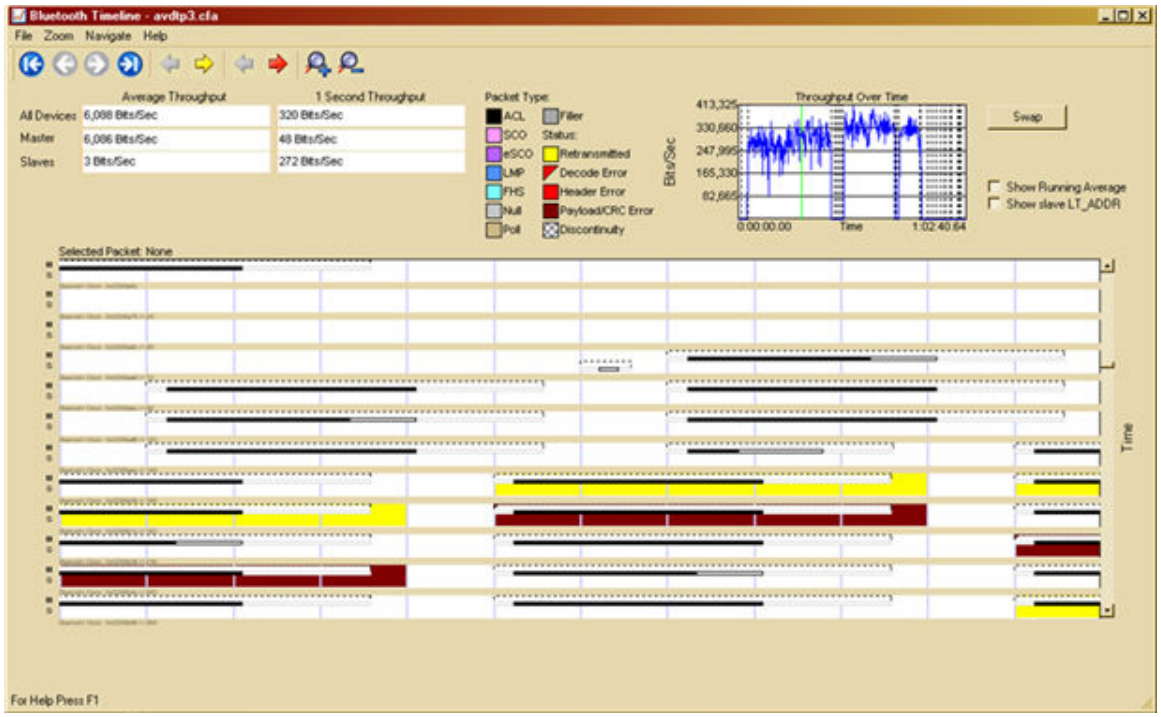
Only channels with a base value of 5 GHz and spacings of either 20 or 40 MHz are shown here. Due to space limitations, each channel is drawn with a fixed height instead of being sized and spaced relative to its width and distance from other channels (unlike the 2.4 GHz channels - both Wi-Fi and Bluetooth® - which are sized and spaced relative to each other with the exception of Wi-Fi channel 14).

13 Bluetooth Timeline

13.1 Bluetooth® Timeline

In addition to the Coexistence View, which displays both *Bluetooth*® and Wi-Fi data together, you can also see more information about *Bluetooth* in a separate dialog. The *Bluetooth* Timeline displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from the Frame Display and the Protocol Navigator.

The timelines provide a rich set of diverse information about *Bluetooth* packets, both individually and as a range. Information is conveyed using text, color, graphic size, line type, and position.



You access the *Bluetooth* Packet Timeline by selecting **Bluetooth Timeline** from the View menu or by pressing the *Bluetooth* Timeline icon  on the Control Window toolbar, Frame Display, or Protocol Navigator.

Select one of the links below to learn more about the *Bluetooth* Timeline.

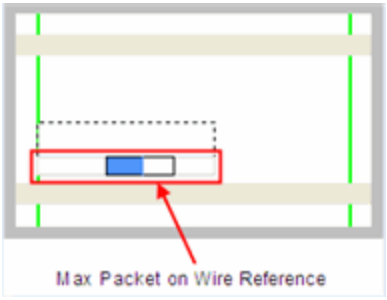
13.2 Bluetooth® Timeline Packet_Depiction

The timeline shows *Bluetooth* packets within a specific period of time.

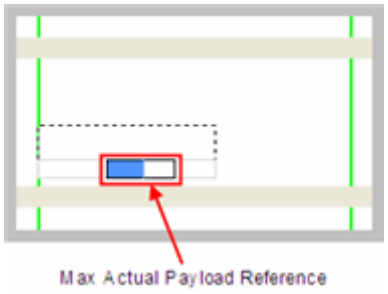
- The timeline shows Bluetooth packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: M (master) and S (Slave). Packets are placed on M or S depending on which type of data it is.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

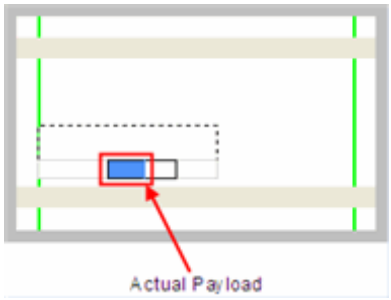
- A "**max packet on wire reference**" rectangle (light solid lines). This indicates the packet on the wire with a max payload.



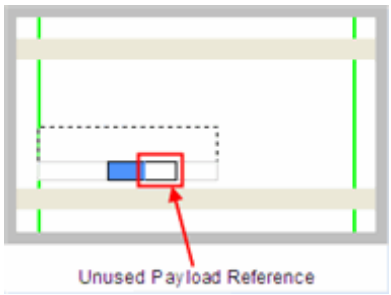
- A "max actual payload reference" rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload on the wire contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates where the payload begins in time.



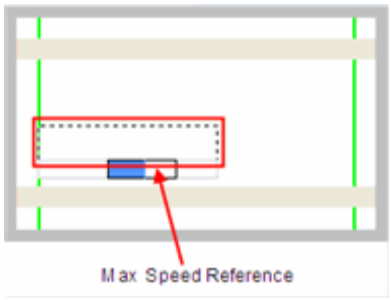
- • An “**actual payload**” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference” rectangle is colored.



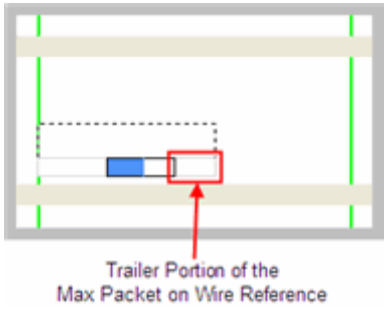
- • An “**unused payload reference**” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet on the wire does not leave room for this. It is indicated for reference only.



- • A “**max speed reference**” rectangle (dashed lines). This is used to extend the height to that of a 3 Mbits/sec packet, and appears only for packets whose speed is less than that. The packet shown here has a speed of 1 Mbit/sec because the height of the other rectangles is 1/3 of the total height.



The part of the “max packet on wire reference” rectangle (light solid lines) that trails the “max actual payload reference” rectangle (dark solid lines) is partly packet on the wire (if the payload on the wire contained FEC) and partly trailer (CRC, etc). There is always a trailer, so there is always a little space (subject to round off error and pixel granularity) between the ends of the two rectangles.



This table shows how packets are colored:

Packet Category	Packet Types	Color
ACL	DM1, DM3, DM5 DH1, 2-DH1, 3-DH1 DH3, 2-DH3, 3-DH3 DH5, 2-DH5, 3-DH5 AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink
eSCO	EV3, 2-EV3, 3-EV3, EV4 EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark blue
FHS	FHS	Light blue
NULL	NULL	Light gray
POLL	POLL	Light brown
Filler	Filler provided by FTS	Dark gray

*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.

This table summarizes the various ways in which packet information is presented:

Information	Text	Color	Graphic size	Position
Packet type	x			
Packet category		x		
Protocol	x	x		
Time of occurrence	x			x
Source device	x			x
Duration			x	
Size in bytes	x		x	
Size as a percentage of max size for that packet type	x		x	
Speed			x	
Status	x	x		

Bluetooth Channel Frequencies

13.3 Bluetooth® Timeline Packet Navigation and Selection

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous error packet, next or previous retransmitted packet (*Bluetooth* only), and the first or last packet.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the Frame Display.
- Selecting Previous Packet with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting Next Packet with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Selecting Previous/Next for a packet that's currently visible selects it without scrolling.
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline, it is also becomes selected in the Frame Display. When multiple packets are selected in the timeline, only one of them is selected in the Frame Display.
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

13.4 Bluetooth® Timeline Button Bar

The button bar contains the following:



Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.

 Unlock

 First Packet

 Previous Packet

 Next Packet

 Last Packet

 Previous Retransmitted Packet

 Next Retransmitted Packet

 Previous Error Packet

 Next Error Packet

 Zoom In - Click on the icon each time to zoom in from 4800 slots to 12 slots

 Zoom Out - Click on the icon each time to zoom out from 12 slots to 4800 slots

 Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in the Frame Display or Protocol Navigator. Resetting the display may be useful when the most recent throughput values are of interest.

13.5 Bluetooth® Timeline Menu Bar

The menu bar contains the following:

File Menu:

Toggle Display Lock
(available only in live mode)

Reset (available only in live
mode)

Exit

Zoom Menu:	**Keyboard Shortcuts:**
Zoom In	Ctrl+Plus
Zoom Out	Ctrl+Minus
Zoom In Tool	
Zoom Out Tool	
Selection Tool	
12 Slots (3 X 4)	
36 Slots (6 X 6)	
144 Slots (12 X 12)	
324 Slots (18 X 18)	
576 Slots (24 X 24)	
900 Slots (30 X 20)	
1296 Slots (36 X 36)	
1764 Slots (42 X 42)	
2304 Slots (48 X 48)	
2916 Slots (54 X 54)	
3600 Slots (60 X 60)	
4356 Slots (66 X 66)	
5184 Slots (72 X 72)	

Navigate Menu:	**Keyboard Shortcuts:**
First Packet	Home
Last Packet	End
Previous Packet	Left Arrow

Next Packet	Right Arrow
Previous Retransmitted Packet	
Next Retransmitted Packet	
Previous Error Packet	Ctrl+Left Arrow
Next Error Packet	Ctrl+Right Arrow
Selected Packet	Enter
Toggle Display Lock (available only in live mode)	L

Help Menu:

Help Topics

About

13.6 Bluetooth® Timeline Visual Elements

The *Bluetooth* Timeline consists of the following visual elements:

- **The timeline shows *Bluetooth* packets within a specific period of time.**
  - The timeline shows Bluetooth packets within a specific period of time.
  - The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
  - Within each row are two divisions: M (master) and S (Slave). Packets are placed on M or S depending on which type of data it is.
  - Placing the mouse pointer on a packet displays information about that packet in an information box.
  - Selecting a packet by clicking on it shows information about that packet above the timeline.
  - You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
  - Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.

- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

- **Rows of *Bluetooth* Slots**

  Each slot begins at the left edge of the vertical blue bar. There are two *Bluetooth* clocks per slot. Each slot represents 0.000625 seconds, or 625 µs.

- **'M' and 'S' labels**

  Within each row, master and slave packets are indicated on the left side of the row. By default, all possible slave devices (there can be up to 7) are put on the 'S' sub-row, but checking the "Show slave LT_ADDR" checkbox shows all existing slave device sub-rows with numbered labels (some or all of S1, S2, …, S7).

- ***Bluetooth* Clock**

  The *Bluetooth* clock of the first slot in each row is shown underneath each row.

- **Packet Info Line**

  The packet info line appears just above the timeline and displays information for the currently selected packet(s). If only one packet is selected, this information consists of the packet number, packet type, *Bluetooth* clock (*Bluetooth* only), and Timestamp. If multiple packets are selected, this information consists of the packet range, the *Bluetooth* clock delta (*Bluetooth* only), and the Timestamp delta. Selected packets are bounded by a magenta rectangle. See the Packet Navigation and Selection section.

- **Floating Information Window (aka Tooltip)**

  The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For *Bluetooth*, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Frame Display (with the percentage of the Payload Length max added), and the decode of the highest layer (if it's not the Baseband layer) as displayed in the Protocol Navigator.

- **Discontinuities**

  Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.

- **Zoom Tools**

  Zoom tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See the "Zooming" section.

- **Packet Status**

Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.

- **Right-Click Menu**

  The right-click menu provides zooming and tool selection. See the "Zooming" section.

- **Graphical Packet Depiction**
  Each packet within the visible range is graphically depicted. See the "Packet Depiction" section.

- **Swap Button**
  The Swap button switches the position of the Timeline and the Throughput graph.

- **Show Running Average**
  Selecting this check box shows a running average in the Throughput Over Time graph as an orange line

- **Show slave LT_ADDR**

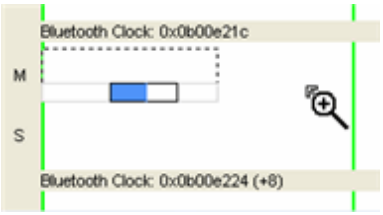
  Selecting this checkbox displays the Slave LT_ADDR in the timeline row labels.

13.7 Bluetooth® Timeline Zooming

Zoom features can be accessed from the Zoom menu, clicking a zoom tool on the toolbar, or by right clicking on the Timeline window.

A couple of things to remember about Zooming.

- Zoom tools accessed using the right click menu allow you to maintain the current position on the screen and precisely zoom in to a specific packet.
- Selecting a Zoom icon (+ or -) on the toolbar does not change the pointer to a Zoom Tool. Each distinct click only zooms in our out.
- Zoom tools accessed from the Zoom Menu have a pointer in the upper-left corner which is useful for specifying the zoom location and bringing up a tool tip of a specific packet.



13.8 Bluetooth® Timeline Throughput Displays

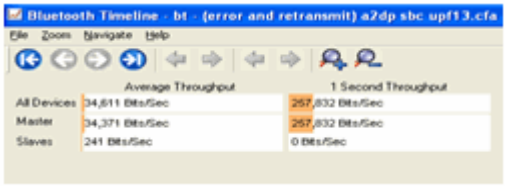
Throughput is payload over time. There are 3 categories of throughput:

- Average
- 1-second
- Graph

In computing throughput, payload is not counted from Bluetooth packets that have a CRC error (dark red slot) or that are a retransmission (yellow slot).

13.9 Bluetooth® Timeline Average Throughput Indicators

The following figure depicts the Throughput display with the Average Throughput indicators in the left column.



Average throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

- Average throughput is shown as 0 when there is only one packet, because in that case the timestamp difference is 0 and an average cannot be computed.
- Average throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

13.10 Bluetooth® Timeline One Second Throughput Indicators

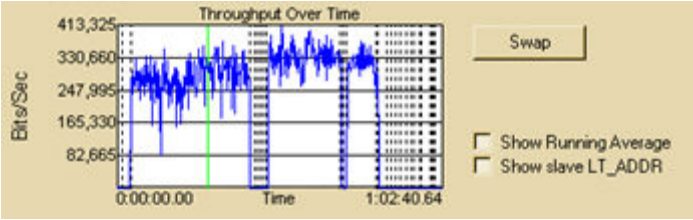
- 1-second throughput is the total payload over the most recent one second of duration (This is determined by counting *Bluetooth* clocks). It is cleared after each discontinuity. A discontinuity is when the *Bluetooth* clock goes forward more than two (2) seconds or goes backwards any amount. This is caused by either a role

switch or *Bluetooth* clock rollover . The *Bluetooth* clock count is used instead of timestamp difference because the *Bluetooth* clock count is precise; however, if timestamp difference were used it would not be necessary to clear the 1-second throughput after each discontinuity.

- 1-second throughput is not an average. It is simply the total payload over the most recent one second of duration. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small payload by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- A 1-second throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

13.11 Bluetooth® Timeline Throughput Graph

The following figure depicts the Throughput Graph (Throughput Over Time).



The throughput graph shows total payload for each successive time interval. The time interval is initially 0.1 second. Each time the number of throughput elements reaches 100, they are collapsed into a set of 50 by combining adjacent elements and doubling the duration of each element. Collapsing thus occurs as follows:

Collapse count	Time since beginning of session (seconds)	Element duration after collapse (seconds)
1	10	0.2
2	20	0.4
3	40	0.8
4	80	1.6
5	160	3.2
6	320	6.4

and so on...

The bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.

Discontinuities are indicated by vertical dashed lines.

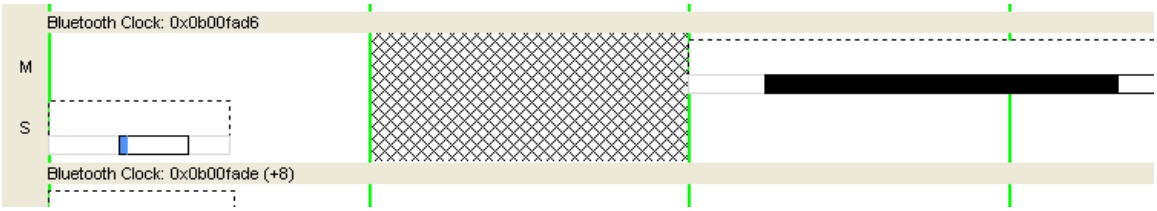
A green view port indicates the time range corresponding to the visible slots in the timeline. The view port can be moved by clicking elsewhere in the graph or by dragging. Whenever it is moved, the timeline scrolls to match. When the slot range in the timeline changes, the view port moves and resizes as necessary to match.

The **Swap** Button
The Swap button switches the position of the Timeline and the Throughput graph.

Show Running Average
Selecting this check box shows a running average in the Throughput Over Time graph as an orange line

13.12 Bluetooth® Timeline Discontinuities

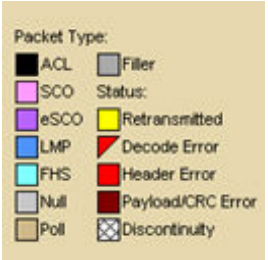
The following figure depicts a Discontinuity between two packets.



To keep the timeline and the throughput graph manageable, big jumps in the Bluetooth clock are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the Bluetooth clock goes forward more than two (2) seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph. The Bluetooth clock can jump forward when capture is paused or when there is a role switch (in a role switch, a different device becomes master, and since each device keeps its own Bluetooth clock, the clock can change radically), and backwards when there is a role switch or clock rollover.

13.13 Legend

This legend identifies the color coding found in the timeline.

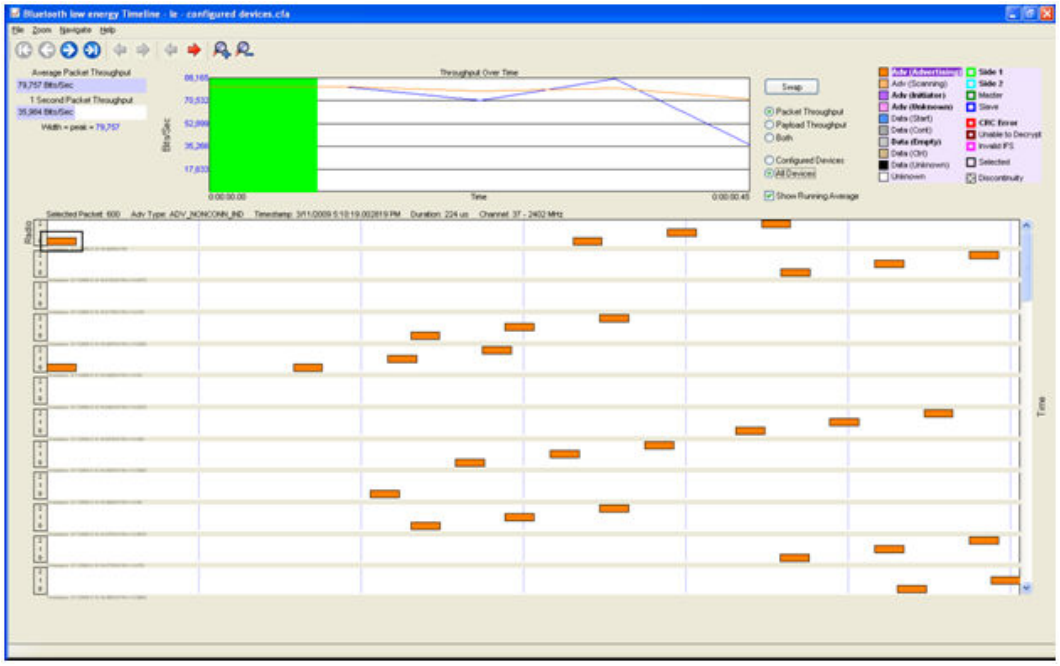


14 low energy Timeline

14.1 low energy Timeline Introduction

The *Bluetooth*® low energy Timeline displays packet information with an emphasis on temporal information and payload throughput. The timeline also provides selected information from the Frame Display and the Protocol Navigator.

The timelines provide a rich set of diverse information about low energy packets, both individually and as a range. Information is conveyed using text, color, packet size, and position.



You access the Timeline by selecting *Bluetooth* low energy Timeline from the View menu or by pressing the *Bluetooth* low energy Timeline icon  on the Control Window toolbar, Frame Display, or Protocol Navigator.

Select one of the links below to learn more about the *Bluetooth* low energy Timeline.

14.2 Bluetooth® low energy Timeline Packet Depiction

The timeline shows Bluetooth packets within a specific period of time.

- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down the to next row, just like reading a book, upper left corner to lower right corner.

- Within each row are three radio possibilities: 2, 1 ,and 0. Packets are placed on 2, 1, or 0 depending on which radio they came in on.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically
- You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet length indicates duration

14.3 Navigating and Selecting Data

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous invalid interframe spacing (IFS), next or previous error packet, and the first or last packet.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the Frame Display.
- Selecting Previous Packet with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting Next Packet with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline it is also becomes selected in the Frame Display. When multiple packets are selected in the timeline, only one of them is selected in the Frame Display.
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

14.4 Button Bar

The button bar contains the following:


Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.


Unlock


First Packet


Previous Packet


Next Packet


Last Packet


Previous Interframe Spacing (IFS) Error

- Interframe Spacing is considered valid if it is within 150 µs + or – 2us
- If the Interframe Spacing is less than 148 us or greater than 152 us but less than or equal to 300 µs, it is considered an IFS error.


Next Interframe Spacing (IFS) Error

- Interframe Spacing is considered valid if it is within 150 µs + or – 2us
- If the Interframe Spacing is less than 148 us or greater than 152 µs but less than or equal to 300 us, it is considered an IFS error.

µs


Previous Error Packet


Next Error Packet


Zoom In - Click on the icon each time to zoom in from 5.0625 s to 7.5 ms.


Zoom Out - Click on the icon each time to zoom out from 7.5 ms to 5.0625 s.


Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in the Frame Display or Protocol Navigator. Resetting the display may be useful when the most recent throughput values are of interest.

14.5 Menu Bar

The menu bar contains the following:

File Menu:

Toolbar

Status Bar

Toggle Display Lock (available only in live mode)

Reset (available only in live mode)

Exit

Zoom Menu:	**Keyboard Shortcuts:**
Zoom In	Ctrl+Plus
Zoom Out	Ctrl+Minus
Zoom In Tool	
Zoom Out Tool	
Selection Tool	
7.5 ms (6 1.25 ms time internals(3x 2))	
22.5 ms (18 1.25 ms time internals (6 x 3))	
90 ms (72 1.25 ms time intervals (12 x 6))	
202.5 ms (1.62 1.25 ms time intervals (18 x 9))	
360 ms (288 1.25 ms time intervals (24 x 12))	
562.5 ms (450 1.25 ms time intervals (30 x 15))	
810 ms (648 1.25 ms time intervals (36 x 18))	
1.1025 s (882 1.25 ms time intervals (42 x 21))	
1.44 s (1152 1.25 ms time intervals 948 x 24))	
1.8225 s (1458 1.25 ms intervals ((54 x 27))	

2.25 s (1800 1.25 ms time intervals (60 x 30))

2.7255 s (2178 1.25 ms time intervals (66 x 33))

3.24 s (2592 1.25 ms time intervals (72 x 36))

3.8025 s (3042 1.25 ms time intervals (78x39))

4.41 s (3528 1.25 ms time intervals (84x42))

5.0625 s (4050 1.25 ms time intervals (90x45))

Navigate Menu:	**Keyboard Shortcuts:**
First Packet	Home
Last Packet	End
Previous Packet	Left Arrow
Next Packet	Right Arrow
Previous Invalid IFS Packet	
Next Invalid IFS Packet	
Previous Error Packet	Ctrl+Left Arrow
Next Error Packet	Ctrl+Right Arrow
Selected Packet	Enter
Lock (available only in live mode)	L

Help Menu:

Help Topics

About

14.6 Visual Elements

The *low energy* Timeline consists of the following visual elements:

- **Rows**
- **Time Markers**

  Time markers indicated by vertical blue lines are shown with a width of 1.25 ms. These are provided to help visualize the timescale and are also useful when using dual-mode chips that do BR/EDR and LE at the same time. Time markers snap to the beginning of the first data packet by default, but they can be snapped to the beginning or end of any packet by right-clicking on a packet and selecting Align Time Marker to Beginning of Packet or Align Time Marker to End of Packet.

- **2, 1, and 0 labels**

  Within each row,2, 1, and 0 radio labels indicate which radio the packet is from.

- **Timestamp**

  The timestamp of beginning of each row is shown underneath each row.

- **Packet Info Line**

  The packet info line appears just above the timeline and displays information for the currently selected packet(s).

  When you select multiple packets, the information includes:

  - Gap = duration between the end of the first packet and the beginning of the last packet.
  - Timestamp Delta = Duration between the beginnings of the first and last packet.
  - Span = Duration between the beginning of the first packet and the end of the last packet

- **Floating Information Window (aka Tooltip)**

  The information window displays when the mouse cursor hovers on a packet. It persists as long as the mouse cursor stays on the packet.

- **Discontinuities**

Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.

- **Zoom Tools**

  Zoom tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See the "Zooming" section.

- **Packet Status**

  Packet status is indicated by color codes. A thick red border indicates a CRC error. A thick dark red border indicates a decryption error. A thick magenta border indicates an invalid IFS.

- **Right-Click Menu.**

  The right-click menu provides zooming and tool selection and time marker alignment.

- **Graphical Packet Depiction**

  Each packet within the visible range is graphically depicted. See the "Packet Depiction" section.

- **Swap Button**

  The Swap button switches the position of the Timeline and the Throughput graph.

- **Show Running Average**

  Selecting this check box shows a running average in the Throughput Over Time graph as an orange line

14.7Zooming

Zoom features can be accessed from the Zoom menu, clicking a zoom tool on the toolbar, or by right clicking on the Timeline window.

A couple of things to remember about Zooming.

- Zoom tools accessed using the right click menu allow you to maintain the current position on the screen and precisely zoom in to a specific packet.
- Selecting a Zoom icon (+ or -) on the toolbar does not change the pointer to a Zoom Tool. Each distinct click only zooms in our out.
- Zoom tools accessed from the Zoom Menu have a pointer in the upper-left corner which is useful for specifying the zoom location and bringing up a tool tip of a specific packet.

14.8 Throughput Displays

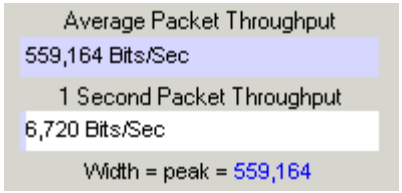
Throughput is payload over time. There are 3 categories of throughput:

- Average
- 1-second
- Graph

In computing throughput, packets that have a CRC error are excluded. (thick red border).

14.9 Packet Throughput

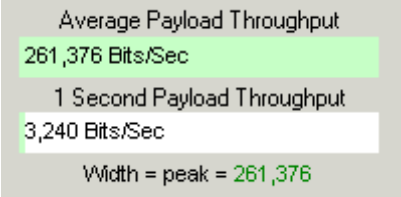
The following figure depicts the Average and 1 Second Packet Throughput displays. This display appears when you select Packet Throughput at the Throughput Graph.



- Average Packet Throughput is the total packet size over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet.
- 1-Second Packet Throughput is the total packet size over the most recent one second of duration.
- Width = peak =: This displays the maximum throughput seen so far.
- A horizontal bar indicates percentage of max seen up to that point, and text gives the actual throughput.

14.10 Payload Throughput

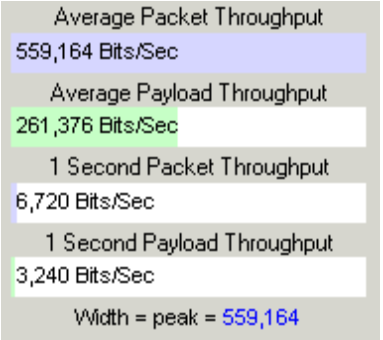
The following figure depicts the Average/ One Second Payload Throughput display. This display appears when you select Payload Throughput at the Throughput Graph.



- Average Payload Throughput is the total payload over the entire session divided by the total time.
- 1-second throughput is not an average. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small packet or payload size by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- Width = peak =: This displays the maximum throughput seen so far.

14.11 Packet/Payload Throughput

The following figure depicts the Average and 1 Second Packet Packet and Payload Throughput displays. This display appears when you select Both at the Throughput Graph.

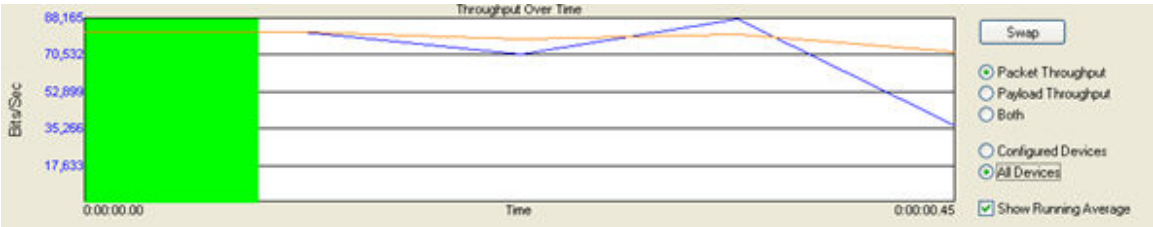


- Average Packet Throughput is the total packet size over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet.
- Average Payload Throughput is the total payload over the entire session divided by the total time.
- 1-Second Packet Throughput is the total packet size over the most recent one second of duration.

- 1-Second Payload Throughput is not an average. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small packet or payload size by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- Width = peak =: This displays the maximum throughput seen so far.

14.12 Throughput Graph

The following figure depicts the Throughput Graph (Throughput Over Time).



The Swap Button

The Swap button switches the position of the Timeline and the Throughput graph.

- Selecting **Packet Throughput** displays just the Packet Throughput in graph form and displays the Average and 1 Second Packet Throughput on the left side of the dialog. The y-axis numbers appear in blue.
- Selecting **Payload Throughput** displays just the Payload Throughout in graph form and displays the Average and 1 Second Payload Throughput on the left side of the dialog.. The y-axis numbers appear in green.
- Selecting **Both** displays both Packet and Payload Throughput. The y-axis numbers appear in blue.
    - Packet Throughput = Blue
    - Payload Throughput = Green
- Selecting **Configured Devices** displays data only from devices that you have configured in Frame Display or where the LA-DATA layer exists.
- Selecting **All Devices** displays data from all available devices.

The bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and is initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.

Discontinuities are indicated by vertical dashed lines.

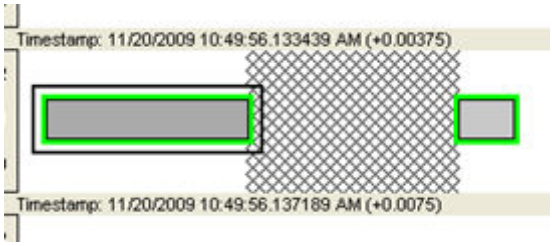
A green viewport indicates the time range corresponding to the visible timeline. The viewport can be moved by clicking elsewhere in the graph or by dragging it. Whenever it is moved, the timeline scrolls to match. When the timestamp range in the timeline changes, the viewport moves and resizes as necessary to match.

Show Running Average

Selecting this check box shows a running average in the Throughput graph as an orange line.

14.13 Discontinuities

The following figure depicts a Discontinuity between two packets.



To keep the timeline and the throughput graph manageable, big jumps in the clock are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the clock goes forward more than 4.01 seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph.

The reason that the discontinuity trigger is set at 4.01 seconds is because the maximum connection interval time is four (4) seconds.

14.14 Legend

This legend identifies the color coding found in the timeline.



- When you select a packet in the timeline, items in the legend that relate to the packet are highlighted.
- A **Bold** highlight indicates that the packet that has been seen in the timeline.

15 Network View

15.1 Network View Introduction

The Network View is a graphic depiction of network nodes and connections between them as indicated by packets received by the analyzer. Information shown includes node statistics, node addresses and names, node pair (i.e. conversation) statistics, and network statistics.

Access the Network View either by selecting *Network View* from one of the *View* menus on other dialogs or by pressing the *Network View* icon  on one of the other dialogs.

The Network View consists of the following dialogs:

- The main Network View dialog
- A Node Database dialog
- An Edit Alias dialog
- A Set Count For Top N Filter dialog

For more information on the Network View, see Network View Technical Notes

15.2 Display Node Information in Network View

The user has complete freedom to specify as many or as few statistics, addresses, and names as are desired and in whatever order is desired. There are ten statistics selections and six name/address selections available for display with each node. Selections to display or remove node information can be made using one of the menus at the top of the dialog (Statistics, Addresses, and Names), or by selecting icons in the toolbar. Select *Show Lines and Dots Only* from the *Format* or right-click menu to hide all node and conversation information in the Detail window, and select it again to display information.

Display:

- Node Statistics

  To display a node statistic in the Detail window, simply select the statistic from the *Statistics* menu or select the appropriate icon from the toolbar. The selected statistic appears at the bottom of the upper list associated with each node in the Detail window. When a statistic is selected, its associated icon appears depressed and its menu item is checked. To remove the statistic from the display, simply select it again. To place the statistic at the top of the node list, press and hold the Ctrl key while selecting the statistic.

  Select from among the following:

  - Bytes Received (BR)
  - Bytes Sent (BS)
  - Bytes Total (BT)

- Nodes In (NI)
- Nodes Out (NO)
- Nodes Total (NT)
- Packets Received (PR)
- Packets Sent (PS)
- Packets Total (PT)
- Utilization (UT)
- Show All Conversations
- Hide All Conversations
- Show Visible Conversations as Bytes (CB)
- Show Visible Conversations as Packets (CB)
- Hide Zero Count Statistics

- Node Addresses

  To display a node address in the Detail window, simply select the address from the *Address* menu or select the appropriate icon from the toolbar. The selected address appears at the bottom of the lower list associated with each node in the Detail window. When an address is selected, its associated icon appears depressed and its menu item is checked. To remove the address from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the address.

  Select from among the following:

  - IP Address (IP)
  - MAC Address (MC)
  - Named MAC Address (NM)
  - Order of Appearance
  - Hide Empty Addresses and Names

- Node Names

  To display a node name in the Detail window, simply select the name from the *Names* menu or select the appropriate icon from the toolbar. The selected name appears at the bottom of the lower list associated with each node in the Detail window. When a name is selected, its associated icon appears depressed and its menu item is checked. To remove the name from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the name.

  Select from among the following:

  - Alias (AL)
  - DNS Name (DN)

- NetBIOS Name (NB)
- Automatically Resolve IP to DNS - You must select this option to use the **Show DNS Names** on the Dashboard
- Hide Empty Addresses and Names

- Node Information Display Options

  In addition to the individual selection options described above, you have several other options for displaying information using the Format menu:

  - Display all node information by selecting *Show All Node Info*
  - Hide all by selecting *Hide All Node Info icon*
  - *Restore Node Info* to return the display to its original state

For a list of node information selections and their corresponding toolbar icons see Network View Toolbar.

15.3 Displaying Conversation Information in Network View

Conversation Statistics

Conversation statistics display on the lines between nodes.

1. Select *Show Info for All Conversations* from the *Format* or right-click menu, or simply click the toolbar icon  .
2. Choose the units to display by selecting *Show Visible Conversation as Bytes* or *Show Visible Conversation as Packets* from the *Statistics* menu..
3. In the event that the Detail window becomes crowded, the conversation statistics may become hidden behind the node statistics display.
4. Select *Put Lines and Conversations On Top* from the *Format* or right-click menu, or click the  icon on the toolbar.
5. Select the menu item again or click the toolbar icon to place the conversation statistics in the background.
6. To hide all conversation statistics, select *Hide Info for All Conversations* from the *Format* or right-click menu, or simply click  on the toolbar.

Quick Tip:

To view statistics for a subset of conversations

- Hover the mouse pointer over the desired node conversation to highlight the line (the line turns magenta to indicate selection)
- Right-click and select *Show this Conversation*.
- Select the menu item again to hide the conversation statistics.

15.4 Adding/Editing an Alias for a Node in Network View

Specifying aliases

An alias is an arbitrary string up to 200 characters in length that the user can define and associate with any MAC address. Each MAC address can have a different alias. Aliases are remembered between sessions and apply to all live captures and capture files. Each alias takes effect as soon as the *OK* button is pressed on the Edit Alias dialog. The Node Database dialog has a Freeze button so that aliases can be added without the dialog's entries moving around.

Add/Edit an Alias

1. Click the *Node Database* icon or select *Node Database* from the *View* menu on the Network View dialog to open the Node Database dialog.
2. Select the row containing the alias you want to add/edit and click the *Edit Alias* button (or simply double click the row) to open the Edit Alias dialog. (Note that during live capture, entries in the Node Database may be moving around, which can make it difficult to select the entry you want. Simply click the *Freeze* button to freeze the display, then click the *Unfreeze button* when you are finished.)
3. Add/edit the alias in the text box and click *OK*.
4. Repeat steps 2 and 3 until all aliases you want to change are completed, and close the Node Database dialog.

Quick Tip:

If you need only add/edit one alias, then hover the mouse pointer over the desired node in the Detail window, right click, and select *Edit Alias* from the menu to open the Edit Alias dialog.

15.5 Filter and Sort the Network View

Filtering:

The *Filter* menu and the tabs above the detail window set the current filter. The filter is always applied to the current sort. Changing the sort criterion may change which nodes are filtered in and which are filtered out.

- **Unfiltered**

  Shows all nodes.

- **No Broadcasts**

  Hides the broadcast node and its conversation lines (i.e. the orange dot and all orange lines disappear).

- **Top N [*Sort by* selection]**

  This shows the top N nodes or conversations based on the statistic listed on the tab (the current sort). The "N" value defaults to 10, but can be set to any value.

- **Top N [*Sort by* selection], No Broadcasts**

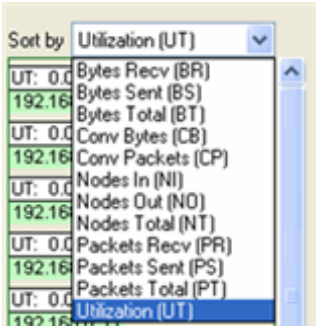
  Hides the broadcast node and its conversation lines, then displays the top N of the remaining nodes or conversations based on the statistic listed on the tab (the current sort). The value of N is the same value used in the Top N filter.

- **Always Shown**

  This shows all nodes that have been marked via the right-click menu as being always shown. The right-click menu makes it possible to specify that the current node, the current node pair (if the mouse cursor is on a conversation line), or all currently selected nodes always be shown (those selected nodes retain this attribute even after they're unselected). The *Undo "Always Shown" For All Nodes* icon  in the toolbar, along with selections in the right-click and *Format* menus, removes this attribute from all nodes. Marking a node as always shown not only ensures that it is always visible regardless of which filter is in effect (inclusion mode), but also makes it possible to isolate nodes by clicking on the Always Shown tab (isolation mode). When a node is visible solely because it's always shown, a little white dot is drawn in the center of it. Thus an always shown node is always visible when the top N filter is in effect, but only when it is not in the top N does it contain a white inner dot. In this way a node's statistics and whether it is in the top N can be monitored simultaneously.

Sorting:

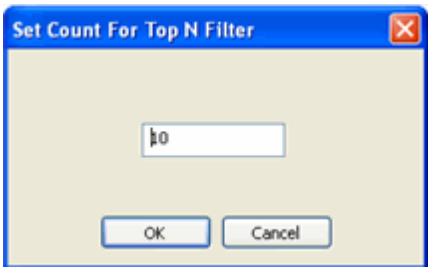
In the Network View, one sort or another is always in effect. Select the statistic to sort on from the *Sort by* drop-down box above the Statistics Graph. The sort in effect is displayed on the Top N tabs and in the Statistics Graph in descending order. The sort order determines which nodes appear in the Detail window when one of the Top N filters is applied.



15.6 Setting The Count For Top N Filters

The Set Count for Top N Filters is an option on the Network View.

1. Click the *Set Count For Top N Filter* icon  , or select *Set Count For Top N Filter* from the *Format* menu to display the Set Count For Top N Filter dialog.



2. Enter a new value for N and click *OK*.

The new value of N appears on the Top N filter tabs on the Detail window.

15.7 Detail Window Layouts in Network View

There are three layout possibilities for the Detail window, each of which provides a different degree of flexibility. Layouts are selected from the Format menu or by selecting icons on the toolbar. Select *Use Black Background* from the *Format* or right-click menu to display a black background in the Detail window.

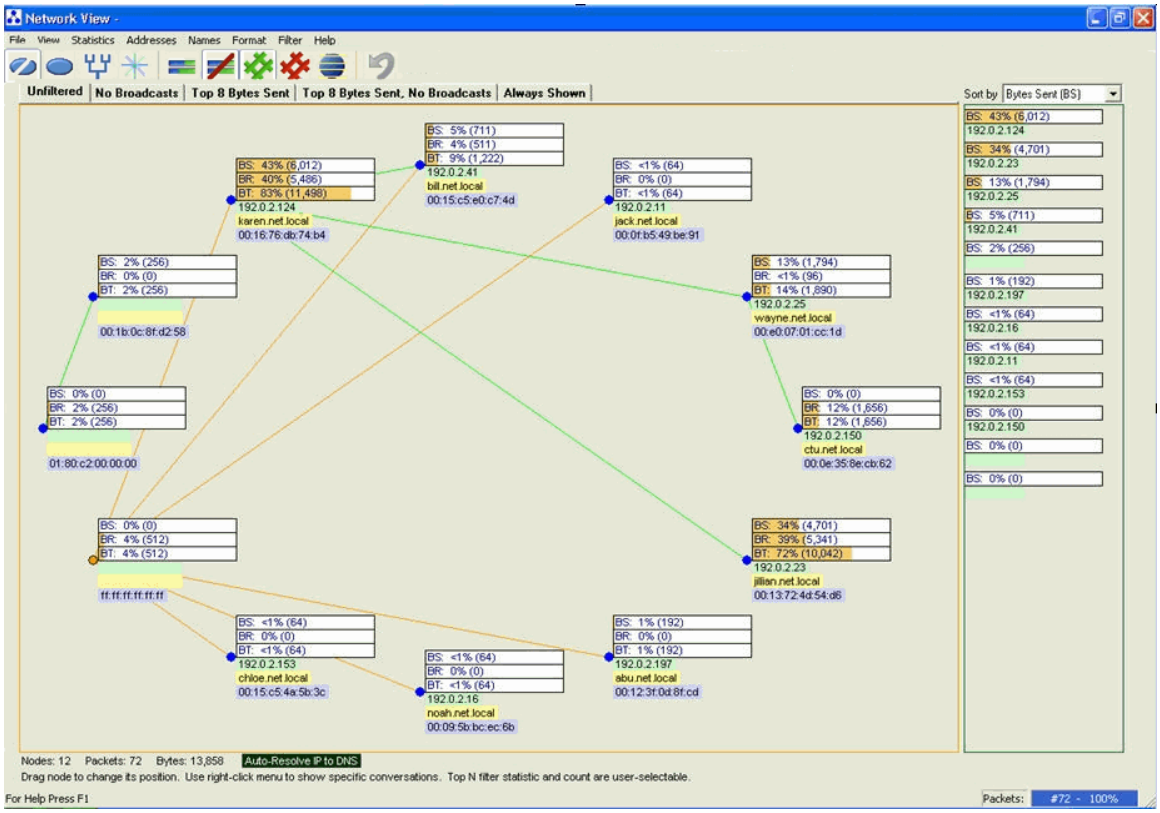
- **Exploded Oval Layout**

  Exploded Oval Layout shows nodes evenly arranged in an oval shape in the Detail window. Click the *Exploded Oval Layout* icon  or select *Exploded Oval Layout* from the *Format* menu to display this layout.

- **Oval Layout**

  Oval Layout also shows nodes in an oval, but instead of arranging them evenly around the oval it leaves gaps where nodes have been filtered out. Since nodes don't move (except for the slight rotation around the oval that occurs each time a new node is discovered and added), this makes it easy to see nodes appear and disappear as they are filtered in and out. On the other hand, it can be more congested than Exploded Oval Layout and thus harder to read. Click the *Oval Layout* icon  or select *Oval Layout* from the *Format* menu to display this layout.

Network View Main Dialog with Oval Layout:

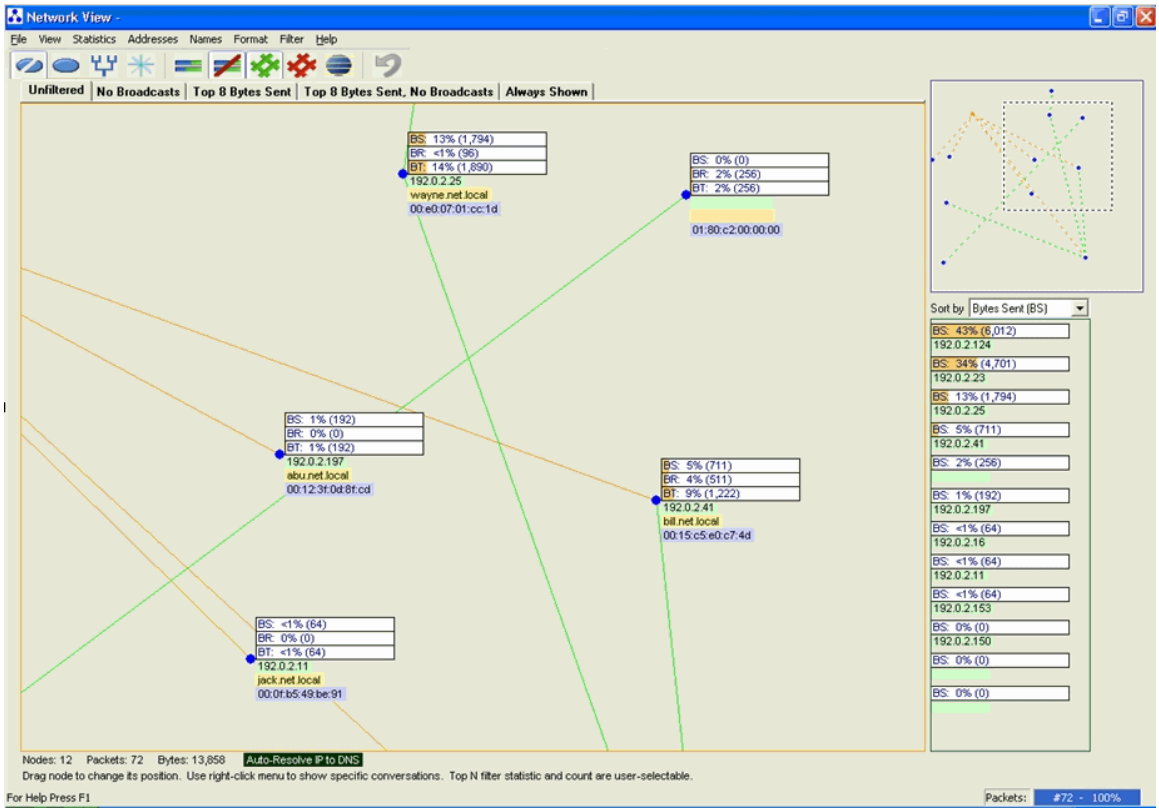


Both Exploded Oval Layout and Oval Layout leave gaps for nodes that the user has dragged (see *Positioning Nodes in the Detail Window* below). In both of those layouts, the oldest node is at the far right and halfway up the detail window (i.e. at the 3 o'clock position). The next oldest node is just above it, and the newest node is just below it. When a node appears for the first time, it is placed just below the oldest node, and the other nodes rotate clockwise around the oval.

- **Branched Layout**

  Branched Layout shows nodes in a free format, and also shows an Overview window which contains a zoomable and movable viewport that can be used to focus the Detail window on a specific area of the network. Branched Layout assigns node positions randomly. Click the *Branched Layout* icon  or select *Branched Layout* from the *Format* menu to display this layout.

Network View Main Dialog with Branched Layout:



Positioning Nodes in the Detail Window

- **Oval Layouts**

  Nodes can be selected and dragged in either Oval layout. A dragged node is not auto-located in either of the Oval layouts, so it provides a means in those layouts for a user to freeze the position of a node. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. Dragged nodes can be moved back into the oval of the current Oval layout by clicking the *Move Dragged Nodes Back Into Oval* icon  or by selecting *Move Dragged Nodes Back Into Oval* from the *Format* menu.

- **Branched Layout**

  Nodes can be selected and dragged in the Branched layout. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. To see any nodes that have been dragged outside of the Detail window, select *Reformat Branched Layout* from the *Format* menu to re-position all nodes within the window.

15.8 The Statistics Graph Window in Network View

The Statistics Graph window displays, in list format, a subset of the node or conversation information displayed in the Detail window. This window is always sorted in descending order of the statistic displayed. The statistic that appears in this window can be one of ten Node statistics, or one of two Conversation statistics, and is user controlled.

- **Node Statistics**

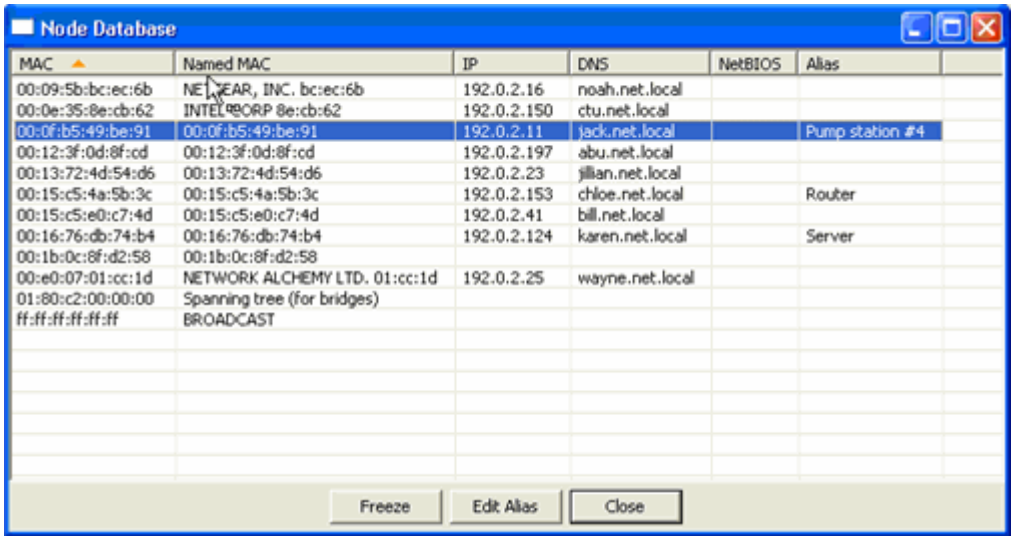
  When a node statistic is chosen as the sort criterion, the Statistics Graph displays the selected statistic and the topmost address/name (as it appear in the Detail window) for each node displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected statistic, its percent value, and its actual value. The only exception is Utilization, where only the actual value is displayed. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

- **Conversation Statistics**

  When either Conversation Bytes (CB) or Conversation Packets (CP) statistic is chosen as the sort criterion, the Statistics Graph displays the selected conversation statistic, and the topmost addresses/names (as they appear in the Detail window) for the corresponding pair of nodes displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected conversation statistic (CB or CP), its percent value, and its actual value. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

15.9 The Network View Node Database

The Node Database dialog shows node addresses and names in a sortable table. It is kept up-to-date with the Network View main dialog at all times unless the Freeze button on the Node Database dialog has been pressed, in which case no new rows are added (individual fields within each entry are still updated however). The purpose of the Freeze button is to keep the table entries in one place while the user is in the process of adding aliases. The display can be sorted on any column in ascending or descending order simply by clicking on the column header. The sort in effect, and the direction of the sort, is indicated by a pointer in the column header. The sorted column is sorted such that blank entries always appear at the bottom of the column.



15.10 Resolving DNS Names in Network View

IP addresses are resolved to DNS names in two ways: automatically or manually. Resolution is achieved via network query, and is the only instance in which the Network View places a message on the network. In auto-mode, at most one resolution is attempted per second to ensure that Network View-generated traffic is minimal. Other processing continues while this resolution is underway.

- **Resolve DNS Names Automatically for All IP Addresses**

  Select *Automatically Resolve IP To DNS* from the *Names* menu or from the right-click menu.

  A check mark appears next to the menu item and the text *Auto-Resolve IP to DNS* appears in the Status line just below the Detail window.

  To stop auto-resolve, simply select (un-check) the menu item again.

- **Resolve DNS Names Manually for Individual IP Addresses**

  If you need only resolve one or two IP addresses, then hover the mouse cursor over the desired node in the Detail window and select *Resolve IP to DNS* from the right-click menu. Once resolution is complete, the DNS for the selected node appears in the node's list (ensure that DNS Name is selected as a list item).

15.11 The Network View Toolbar

The toolbar contains the following:


Exploded Oval Layout - Displays the Exploded Oval Layout in the Detail window


Oval Layout - Displays the Oval Layout in the Detail window



Branched Layout - Displays the Branched Layout in the Detail window



Move Dragged Nodes Back Into Oval - Moves any nodes that were dragged from their original positions back to those positions.



Show All Conversations - Shows all conversation statistics in the Detail window.



Hide All Conversations - Hides all conversation statistics in the Detail window.



Put Lines and Conversations On Top - Displays lines and conversation statistics on top of nodes and node information (statistics, addresses, and names) in the Detail window.



Undo Always Shown For All Nodes icon - Removes the *Always Shown* attribute from all nodes.

15.12 Network View Visual Elements

The main Network View dialog consists of the following visual elements:

- **The Title Bar**

  The Title Bar shows the name of the current capture file (if any).

- **The Menu Bar**

  The Menu Bar contains pull-down menus with selections for all functions in Network View.

  - File - Allows you to hide/show the Toolbar and Status bar, and also Exit
  - View - Allows you to open the Dashboard, Frame Sizes, and Node Database dialogs
  - Statistics - Allows you to activate/deactivate various statistics
  - Addresses - Allows you to hide/show various address types
  - Names - Allows you to hide/show various name types
  - Format - Allows you to choose between Exploded, Oval, and Branched layouts. Also allows you to hide/show types of data.
  - Filter - Allows you to manage the type and amount of information displayed.
  - Help - Opens the Help files

- **The Toolbar**

  The Toolbar contains buttons for display selection, and frequently used functions.

- **The Detail Window**

  The Detail window displays each node, connections between nodes, various user-selectable statistics and addresses, and mouse hover information windows (aka tooltips). This window has a set of tabs just above it which provide filter selection.

- **The Statistics Graph Window**

  The Statistics Graph window displays a subset of the node information that is displayed in the Detail window in list format. This window displays the statistic selected in the *Sort by* drop-down box located at the top of the window. The Statistics Graph window lists the selected statistic in descending order, along with the topmost Name/Address (as it is displayed in the Detail window).

- **The Overview Window**

  The Overview window provides the ability to scroll and zoom the spatially oriented Branched Layout in the Detail window, and display all or part of the network

  Note: This window appears only in Branched Layout.

- **The Status Line**

  The Status Line appears just below the Detail window, and displays various totals and states.

- **The Instruction Line**

  The Instruction line appears just below the status line, and contains some simple instructions for the user.

The Network View dialog is re-sizable and contains a right-click menu. The “Packets” indicator in the lower-right corner is identical to those on the Control Window and Frame Display.

15.13 Network View Technical Notes

Information Gathering and Processing

- Packets are used to obtain addresses and compute statistics for each node, each pair of connected nodes, and for the network as a whole.
- System query is used to resolve IP addresses to DNS names.
- Aliases are specified by the user.
- Node statistics are saved for each occurrence of each MAC address in each packet. A complete list of node and conversation statistics is given in a table below.
- Conversation statistics are saved for each pair of MAC addresses from each packet, and is direction-specific.

- Network statistics are simply a total of all of the node statistics.
- Since statistics are saved by MAC address, a changing IP address does not change the computed statistics.

Information Storage

The obtained and computed information is saved when a live capture is saved to a capture file. When the capture file is reopened, the stored information is retrieved and used without having to reprocess the packets in the capture file.

Textual and Graphical Representation

Each node is represented as a dot, and one or more conversations between a pair of nodes are indicated by a single line connecting the two corresponding dots. Dots are normally blue and lines are normally green, but broadcasts are shown as orange lines that are connected to a single orange dot that does not represent an actual node and whose sole purpose is to provide a broadcast endpoint.

Node statistics, addresses, and names are displayed to the right of each node in the Detail window. Statistics are displayed above the centerline of the dot that represents the node. Addresses and names are displayed below the centerline.

With the exception of utilization, each statistic is displayed as a little horizontal single-item bar graph which shows the count and percentage as text and uses the bar to graphically represent the percentage. A text prefix and text color-coding indicate which statistic it is (see table below).

Utilization does not show a percentage. Instead, it uses color-coding to indicate its absolute value (see table below).

Addresses and names have color-coded backgrounds: MAC = purple, Named MAC = cyan, IP = light green, DNS = yellow, NetBIOS = blue, and Alias = light red.

There can be any number of statistics, addresses, and names displayed for each node, and these are selected via the icons in the toolbar at the top of the main Network View dialog. The order of display follows the order of selection from top to bottom, except that selecting an icon via a Ctrl-click puts that item at the top of the list instead of at the bottom.

Node or conversation data is displayed in the Statistics Graph depending on the selection made in the *Sort by* combo box above the graph. The entries in the Statistics Graph are sorted by descending statistic value.

Conversation data is displayed along each line that connects two nodes and is direction-specific. Either byte count or packet count can be displayed (this is done via the Format menu, right-click menu, or by selecting the Conversation Bytes or Conversation Packets icons in the toolbar). These statistics are displayed as single-item bar graphs which always hug the line connecting the nodes, rotating as the line is rotated. The statistic text flips as the user moves the line through vertical so that the text is never upside-down. A little arrow at the end of the statistics box indicates the direction of the conversation. The colors in a conversation statistic bar graph (green on blue) are different from the colors in a node statistic bar graph (orange on white) so that it's easy to distinguish between them.

User Defined Settings

User defined settings and display options listed below persist across sessions.

- Layout selection
- Positions of dragged nodes in Oval Layout and Exploded Oval Layout
- Positions of all nodes in Branched Layout
- Filter selection
- *Count for Top N Filter* setting
- Sort order selection
- *Always Shown* node selections
- Node statistics, addresses, and names selected for display
- Conversations displayed and statistic selected
- *Put Lines and Conversations On Top* selection
- Detail window background color selection
- *Show Lines And Dots Only* selection
- Auto-resolve IP addresses to DNS names selection
- Aliases

Node and Conversation Statistics:

Prefix	Type	Bar Graph?	Text Color	Bar Graph Color	Description
BR	Node	Yes	Blue	Orange on White	Bytes Received
BS	Node	Yes	Blue	Orange on White	Bytes Sent
BT*	Node	Yes	Blue	Orange on White	Bytes Total (Bytes Received + Bytes Sent)
NI	Node	Yes	Green	Orange on White	Nodes In
NO	Node	Yes	Green	Orange on White	Nodes Out
NT**	Node	Yes	Green	Orange on White	Nodes Total

PR	Node	Yes	Red	Orange on White	Packets Received
PS	Node	Yes	Red	Orange on White	Packets Sent
PT*	Node	Yes	Red	Orange on White	Packets Total (Packets Received + Packets Sent)
UT	Node	No	See following table	See following table	Utilization (Megabits/Sec over the last 10 seconds, counting both Bytes Sent and Bytes Received)
CB	Conversation	Yes	Blue	Green on Blue	Conversation Bytes
CP	Conversation	Yes	Red	Green on Blue	Conversation Packets

**The Bytes Total and Packets Total statistics each add up to 200% since they count each byte twice, once at the sending node and once at the receiving node.*

*** The Nodes Total statistic counts unique nodes, so it's not simply a sum of nodes sent to and nodes received from. For example if node A sends to only nodes B and C and receives from only node B, its total node count is 2, not 3.*

Here is utilization coloring:

Utilization (Megabits/Second)	**Colors**
<0.01	Black on White
>= 0.01 and < 2	White on Dark Blue
>= 2 and < 3	Black on Yellow
>= 3	White on Dark Red

Utilization for each node is shown as megabits/second and is computed over the last 10 seconds, even if the node has been present for less time than that. Both bytes sent and bytes received are counted, so if there are only two devices A and B on the network and all that is

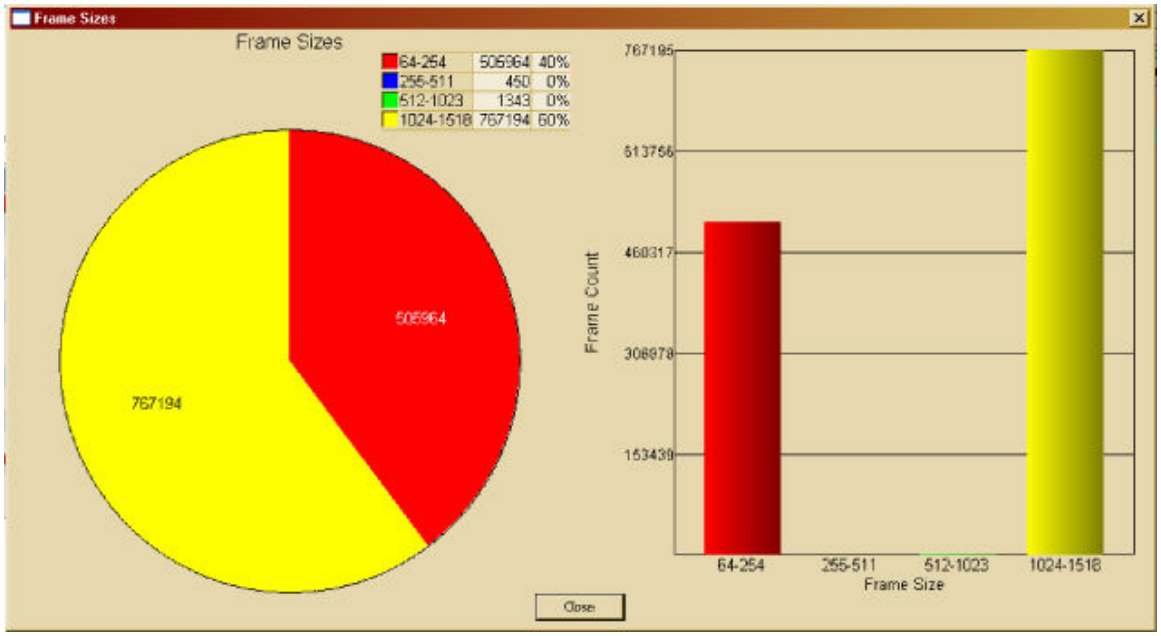
happening is that device A is sending to device B, both of those devices display the same utilization.

A mouse hover information window (aka tooltip) showing all statistics, addresses, and names can be displayed for each node. The tooltip background is normally yellow, but since the nodes can move, the tooltip background turns green and the text "*** Node not under mouse pointer" appears at the bottom of the tooltip when the node moves out from under the mouse pointer or disappears altogether. The tooltip itself, however, persists until the user moves the mouse pointer or presses Esc. The tooltip regains its original yellow appearance if the node moves back under the mouse pointer.

15.14 Network View - Frame Sizes

The Frame Sizes window is accessed from the Network View > View menu.

The window displays the percentage of captured data in four byte size ranges: **64-0254**, **255-511**, **512-1023**, and **1024-1518** in a pie chart and a vertical graph.



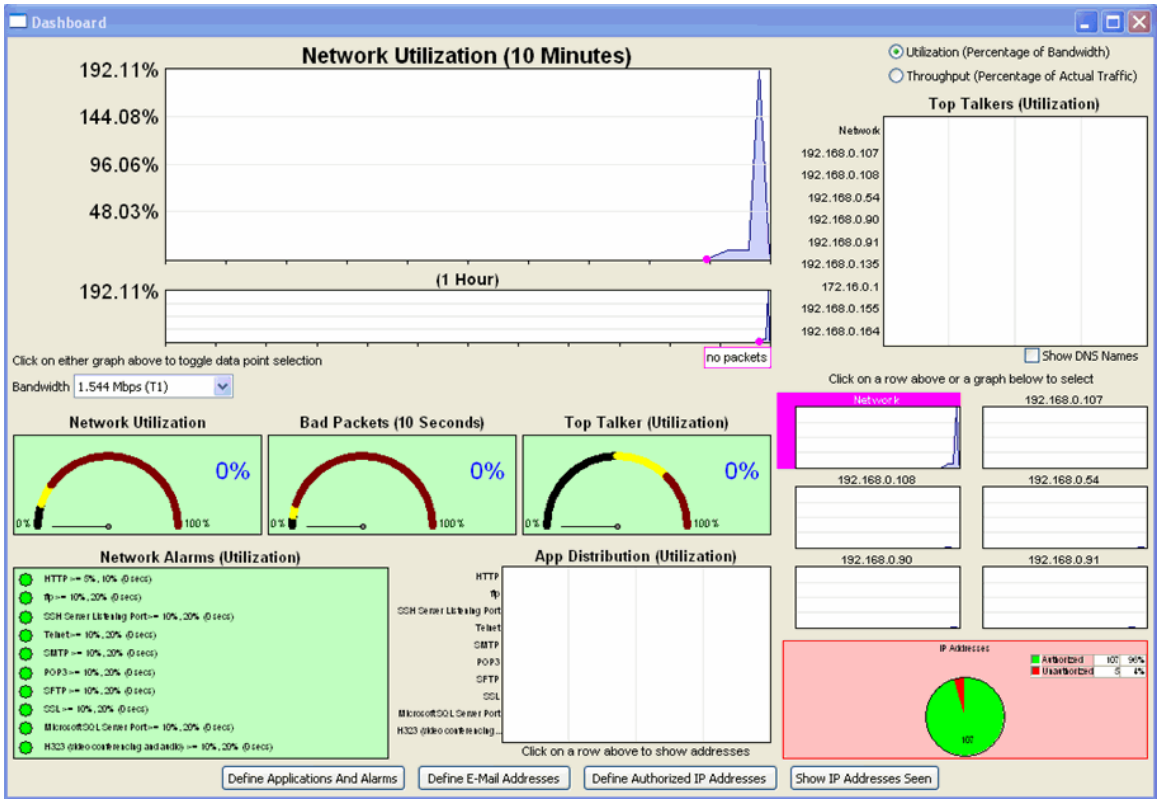
The window is a display only. There is no user interaction.

16 NetDecoder Dashboard

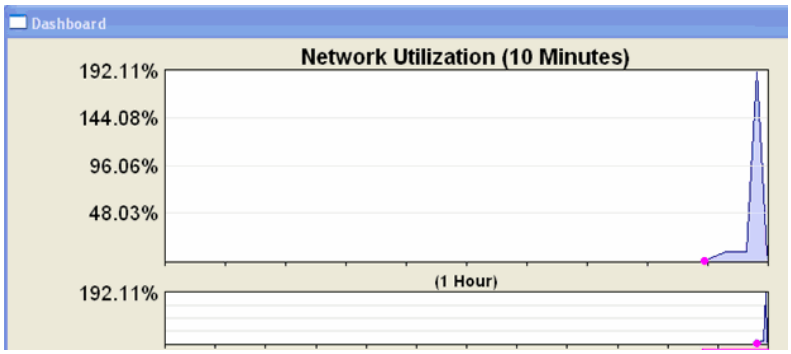
16.1 Dashboard

NetDecoder's new Dashboard View displays a dynamic view of what is occurring on your Ethernet communications network.

You access the Dashboard by selecting Dashboard from the View Menu on the Control Toolbar and Network View windows or from the Dashboard icon  on the Control Window and Frame Display Toolbars.



16.1.1 One Hour/Ten Minute Chart

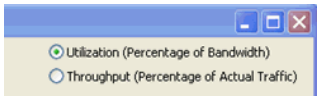


These graphs displays the activity for the last one (1) hour/ten minutes for an IPaddress or DNS Name selected on the Top Talkers (Utilization) or Top Talkers (Throughput) bar chart. Clicking on an IP address in the chart changes the graph.

A pink dot appears when you click on the bottom of the graph. The dot synchronizes between the One Hour/Ten Minutes charts..

A black dot appears when you select a point on the graphs.

16.1.2 Dashboard: Utilization (Percentage of Bandwidth) and Throughput (Percentage of Actual Traffic)



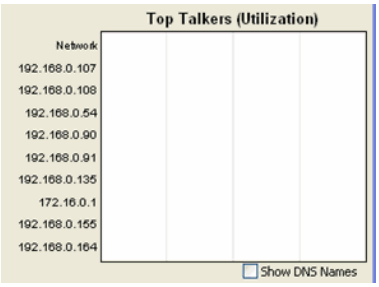
On the Dashboard, selecting the **Utilization (Percentage of Bandwidth)** button affects several areas of the Dashboard:

- Top Talkers Utilization/Top Talkers Throughput Graph - Displays utilization expressed as % bandwidth. Shows for network and each device in descending order. Max 10 entries.
- Bad Packets (10 Seconds)/Bad Packets Meter - Displays % bad packets over last 10 seconds.
- Top Talker Utilization/ Top Talker (Throughput) - Displays utilization expressed as % bandwidth for device with highest utilization.
- Application Distribution Utilization/Application Distribution (Throughput) - Displays utilization expressed as % max bandwidth per specified app for last 10 seconds or since app was defined, whichever is less. Show apps in definition order.

Selecting **Throughput (Percentage of Actual Traffic)** affects several areas of the Dashboard:

- Top Talkers Utilization/Top Talkers Throughput Graph - Displays bytes sent since beginning of session of each device in descending order. Max 10 entries.
- Bad Packets (10 Seconds)/Bad Packets Meter - Displays %bad packets since beginning of session.
- Top Talker Utilization/ Top Talker (Throughput) - Displays percentage of bytes sent since beginning of session for device with highest bytes sent count.
- Application Distribution Utilization/Application Distribution (Throughput) – Displays percentage of bytes sent and received since the app was defined. Shows the apps in definition order.

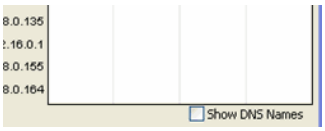
16.1.3 Top Talkers Bar Chart



This bar chart displays bytes sent since beginning of session of each device in descending order with a maximum of 10 entries when the Throughput (Percentage of Actual Traffic) radio button is selected.

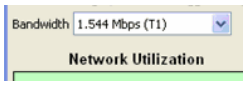
The chart displays utilization expressed as % bandwidth with a maximum of 10 entries when the Utilization (Percentage of Bandwidth) radio button is selected.

16.1.4 Show DNS Names



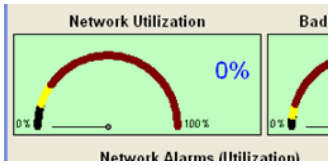
Selecting the Show DNS Names checkbox changes the IP Address displayed in the Top Talkers (Utilization)/Top talkers (Throughput) bar chart to a DNS name. If the DNS name is not available, the IP address is displayed. In order for the DNS name to be available, you must activate Automatically Resolve IP to DNS from the Names menu on the Network View.

16.1.5 Bandwidth Drop-down



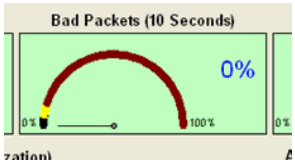
With the drop-down box you can select to view the maximum bandwidth of 1 Gigabyte per second (1 Gbps), OC-3 (155 megabits per second), 100 megabytes per second (100 Mbps), T-3 (43.232 megabits per second), 10 megabytes per second (10 Mbps), and T-1 (1.544 megabits per second).

16.1.6 Network Utilization Meter



Displays the utilization of all devices expressed as % of bandwidth

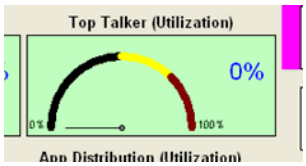
16.1.7 Bad Packets Meter



The Bad Packets (10 Seconds)/Bad Packets Meter displays two different sets of data depending on whether the Percentage of Max Utilization radio button or Percentage of Bytes radio button is selected.

- Utilization (Percentage of Bandwidth) - Displays the % bad packets over last 10 seconds.
- Throughput (Percentage of Actual Traffic) - Displays the % bad packets since the beginning the session.

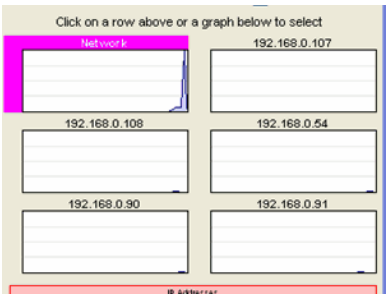
16.1.8 % Top Utilization/Top Utilizer Meter



The Top Talker (Utilization)/Top Talker (Throughput) displays two different sets of data depending on whether the Utilization (Percentage of Bandwidth) radio button or Throughput (Percentage of Actual Traffic) radio button is selected.

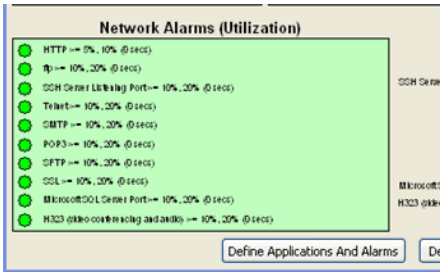
- Top Talker (Utilization) - Shows utilization expressed as % of bandwidth for device with highest utilization.
- Throughput (Percentage of Actual Traffic) - Shows percentage of bytes sent since beginning of session for device with highest bytes sent count.

16.1.9 Charts



These charts displays the Network and top five Top Talkers or Top Utilization IP Addresses from the chart directly above.

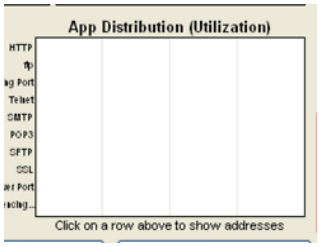
16.1.10 Network Alarms (Utilization)



This chart displays the network alarms configured in the Define Applications and Alarms (Utilization).

- If the data does not exceed the alarms configuration, the tables displays green.
- If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog.
- If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog.

16.1.11 App Distribution (Utilization/Throughput)

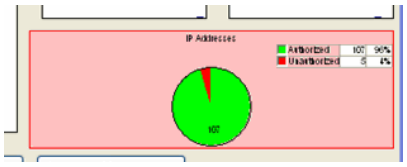


When you select Utilization (Percentage of Bandwidth) radio button, the chart displays the utilization expressed as % bandwidth per specified app for last 10 seconds or since the app was defined, whichever is less. It shows the apps in definition order.

When you select Throughput (Percentage of Actual Traffic) radio button, the chart displays the percentage of bytes sent and received since the app was defined. It shows the apps in definition order.

When you click on an application title on the left side of the chart (or right click in the chart), a dialog appears that displays the address for the application.

16.1.12 IP Addresses



IP Addresses displays the number of authorized IP Addresses in green and the numberof unauthorized IP Addresses in red.

Four buttons at the bottom of the page provide additional options for defining and viewing data.


Click on a row above to show addresses
Define Applications And Alarms
Define E-Mail Addresses
Define Authorized IP Addresses
Show IP Addresses Seen

16.1.13 Dashboard - Define Applications and Alarms

The Applications and Alarms window is used to specify which ports are displayed in the Applications Distribution graph and the Network Alarms (Utilization) table.

1. On the Dashboard select the Define Applications and Alarms button.
2. Select Active App if you want the port to appear in the Applications Distribution graph.
3. Select Active Alarm if you want the port to appear in the Network Alarms (Utilization) table.
4. Enter a name for the port in the Application Name text box.
5. Enter the port number in the Port text box.
6. Select TCP, UDP, or Both from the combo box for the Port Type.
7. Enter a value for the low (Yellow) threshold for the Alarm Threshold (Utilization).

Note: The value of the Yellow threshold is the % of Max Utilization.

If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example, if you set a Yellow threshold of 10% for HTTP and the activity equals or exceeds 10%, the background and circle next to HTTP turns yellow and e-mail is sent indicating a Yellow alarm condition.

8. 8. Enter a value for the high (Red) threshold for the Alarm Threshold (Utilization).

Note: The value of the Red threshold is the % of Max Utilization.

If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example if you set a red threshold of 15% for HTTP and the activity equals or exceeds 15%, the background and the circle next to HTTP turns red and e-mail is sent indicating a Red alarm condition.

When the alarm clears (i.e. the data returns to a Green condition from either a Yellow or Red condition), the background and the appropriate circle turn green and e-mail is sent indicating that the alarm has cleared.

9. Enter a value (in seconds) for a minimum alarm condition duration.

This value identifies how long an alarm threshold must be equaled or exceeded before the alarm is indicated in the Network Alarms (Utilization) table and e-mail is sent. For example, let's say HTTP has a Yellow Alarm Threshold of 10%, with a Min Duration (secs) of 5. This means that the Alarm Threshold of 10% must be equaled or exceeded for at least five seconds for the alarm to show as yellow on the Network Alarms (Utilization) table and for e-mail to be sent.

10. Select Save.

If there are any errors in the settings a message is displayed listing each error. If there are no errors, the settings are saved.

16.1.14 Define Email Addresses

The **Define Email Addresses** window is used to enter email addresses that receive a message when an alarm condition is met or when an unauthorized IP address is detected on the NetDecoder Dashboard. There are two pieces of information you have to enter: mail server and email addresses.

1. On the Dashboard select the *Define Email Addresses*
2. Enter the *Mail Server* address.

To locate the Mail Server address in Outlook:

> Tools > Options > Mail Setup > E-mail Accounts > Data Files > Click on Mailbox - [Name] > Settings > General.

The **Microsoft Exchange server:** field contains the Mail Server address.

3. Enter one or more e-mail addresses

You can only have one email address per line. For multiple addresses, select Enter at the end of the line to move down.

4. Select *Send Test Message* to send a test message to the email addresses.

Once you verify that the mail server and email addresses have been entered correctly:

5. Select *Save.*

When a threshold is exceeded or an unauthorized IP address is seen, an email is sent to the email addresses.

16.1.15 Dashboard - Define Authorized IP Addresses

The Authorized IP Addresses window is used to specify which IP addresses are considered to be either authorized or unauthorized. These IP addresses are the source and destination addresses identified in packets during an analysis.

- Authorized IP addresses are specified in the top section. If this section is selected, all other IP addresses are considered unauthorized.
- Alternatively, unauthorized IP addresses can be specified in the bottom section. If this section is selected, only these IP addresses are considered unauthorized, and all other IP addresses are considered authorized.
- If an unauthorized IP address is detected, an e-mail warning is generated.

By default, all IP addresses are considered authorized.

A count of authorized and unauthorized IP addresses are indicated in the IP Addresses pie chart. The actual addresses are listed in the Show IP Addresses Seen dialog.

To enter an authorized IP address:

1. Select the Authorized IP Addresses radio button.
2. Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
3. Select Save

To enter an unauthorized IP address:

1. Select the Unauthorized IP Addresses radio button.
2. Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
3. Select Save

There are several items to remember when entering authorized or unauthorized IP addresses.

- You can enter one IP address per line.
- The last number in an IP address can be replaced by a dash-separated range (for example 192.168.0.10-20) or an asterisk (for example 192.169.0.*, which is equivalent to 192.169.0.0-255)
- E-mail is sent for the first occurrence of each IP address which is either in the unauthorized list or not in the authorized list (whichever list is selected).

16.1.16 Dashboard - Show IP Addresses Seen

The Authorized IP Addresses Seen window displays which IP addresses have been detected in packets. These packets can either be sent or received.

- Authorized IP addresses are shown in the top section.
- Unauthorized IP addresses are shown in the bottom section.

You specify whether an IP address is authorized or unauthorized using the Define Authorized IP Addresses dialog.

A count of authorized and unauthorized IP addresses detected are indicated in the IP Addresses pie chart. Authorized IP addresses detected are indicated in green. Unauthorized IP addresses detected are indicated in red.

Note: More than just a static display, you can copy and paste IP addresses from both the authorized and unauthorized sections of the dialog into the Define Authorized IP Addresses dialog.

17 Audio Extraction

17.1 Audio Extraction

The Audio Extraction  Plugin allows the user to export Audio data from a SCO or eSCO session to a .wav file. This .wav file can then be played with any standard audio player like Windows Media Player.

You can export the audio data from a capture file with the Export .wav File menu command, or you can Enable Live .wav File Creation and have the data exported as it is captured. The following formats are supported:

- A-Law
- μ-Law
- CVSD

17.2 Audio Extraction Settings

This dialog appears when the user selects Audio Extraction Settings, Export WAV File or Enables Live WAV File Creation.

The following settings are allowed for Audio Extraction:

- The Path where the files are saved.
- The base filename for the WAV files. See File Naming for details on how the files are named and for defaults.
- A choice between one stereo or two mono files for each session.
- A choice between exporting raw or Linear PCM for each type. CVSD are always converted to Linear PCM. You may choose to convert to Linear PCM since more media players accept this format.

17.3 Enable Live WAV File Creation

This menu item exists when the analyzer is live. When this menu item is selected the Settings Dialog appears giving the user the chance to change the settings. WAV files are then created exporting the SCO sessions as they are captured. A Status Dialog appears giving the status of the export operation. The status dialog disappears when if the user disabled Live WAV File Creation.

17.4 Export WAV File

This menu item exists when a file is loaded. When the user selects this menu item a Settings Dialog appears allowing the user to select filenames and other properties.

After the dialog is closed, a window appears giving the Status of the export operation. After the export is finished the dialog disappears.

17.5 File Naming

Audio Extraction creates one or more WAV files that contain the Audio Extraction.

The filenames of the WAV files are based off of the base file name. The base filename and path default to the name and path of the capture file without the extension. The filenames are created like this:

- A "B" is appended to the base filename if stereo mode is on, and "M" or "S" is appended representing, the Master and Slave channels, if it is a mono file.
- The SCO Handle in Parentheses is appended.

Example:

Base file name "Jabra Headset test by fred" produces

- "Jabra Headset test by fred M (1).wav"
- "Jabra Headset test by fred M (20).wav"
- "Jabra Headset test by fred S (1).wav"
- "Jabra Headset test by fred S (20).wav"

17.6 Status Dialog

This dialog appears anytime that Audio Extraction is being exported to a file or being played live. It provides important information like:

- Whether we are exporting a SCO session or waiting for a new one.
- Whether we are exporting to Stereo or Mono.
- Names of Files if they exist.
- Audio Input Format.
- Audio Output Format.
- SCO Handle.
- Current Frame being processed, and percentage complete.

The status window disappears once a capture file has been completely written or if a user disables live extraction. You can also close the status window with the Close button and bring it up at anytime with the "Show Status Window" menu item. The "Show Status Window" also allows the user to bring the status window to the front.

18 Data Extraction

18.1 Data Extraction

The Data Extraction  plug-in allows you to extract files that were transferred over various protocols. You can also choose to have the files opened automatically as long as you have applications able to read the files.

To extract data, select the Extract Data menu item from the View menu on the Control window. When you select this item a settings dialog appears that allows you to define how the system extracts the data.

A status dialog displays the progress and important information concerning the extraction.

18.2 Data Extraction Settings

The Data Extraction  plug-in allows you to extract files that were transferred over *Bluetooth*® protocols.

The following settings appear on the Data Extraction Settings Dialog:

- **Select Profile** – This allows you to select all of the profiles from which to extract data.
- **Path** – This is the path where the files are created.
- **Base File Name** – Certain Profiles like BPP, are not required to have the file name. If the file name does not exist then the name of the file comes from this field.
- **Open File(s) After Extraction** – Select this item if you want the files to open automatically after they are created.

19 Find

19.1 Starting a Search

You can search your data in several different ways. Some types of searches are relevant only for framed data and is not offered if the data is not framed. Other types of searches are available depending on the type of data being viewed.

To Begin a Search

1. Open a capture file, or capture some data to search.
2. Open the Event Display  or Frame Display  window.
3. Click on the *Find* icon  or choose *Find* from the *Edit* menu.
4. The Find window has a tab for each type of search. Click on the appropriate tab for the type of search you want to do.
5. Select the parameters for your search, and click *Find Next*. *Find Next* looks for the next occurrence of the search criteria, while *Find Previous* looks for an earlier occurrence of the search criteria.
6. Press F3 to repeat the last search.

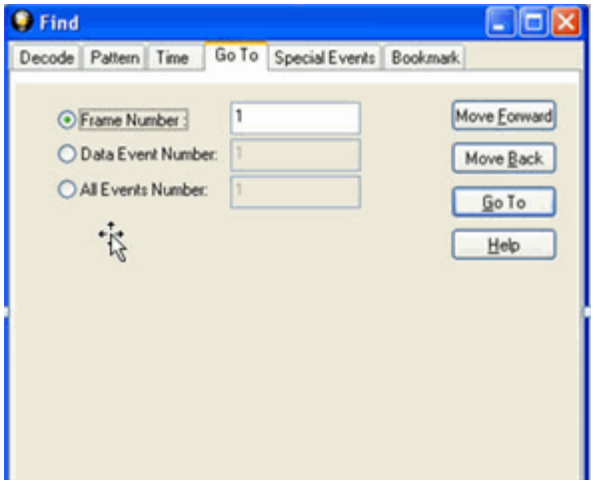
Search results are highlighted in the Event or Frame Displays, or both if appropriate. The selection in the Event Display appears on the third line down from the top of the window by default: this value can be changed.

19.2 Using Go To

This type of search allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Select *Go To* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon  on the toolbar
2. The system displays the Find dialog with the Go To tab selected.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

To go to a particular frame :

1. Select the *Frame Number* radio button
2. Type the frame number in the box.
3. Click the *Go To* button.
4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the *Move Forward* or *Move Back* button.

To go to a particular event :

1. Select the Data Event Number or All Events Number radio button.
2. Type the number of event in the box.
3. Click the Go To button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the Move Forward or Move Backward button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on Move Forward. Each time you click on Move Forward, FTS moves forward 10 events.

See Event Numbering for why the Data Event Number and All Events Number may be different. As a general rule, if you have the Show All Events icon depressed on the Event Display window or Frame Display Event pane, choose All Events Number. If the Show All Events button is up, choose Data Event Number.

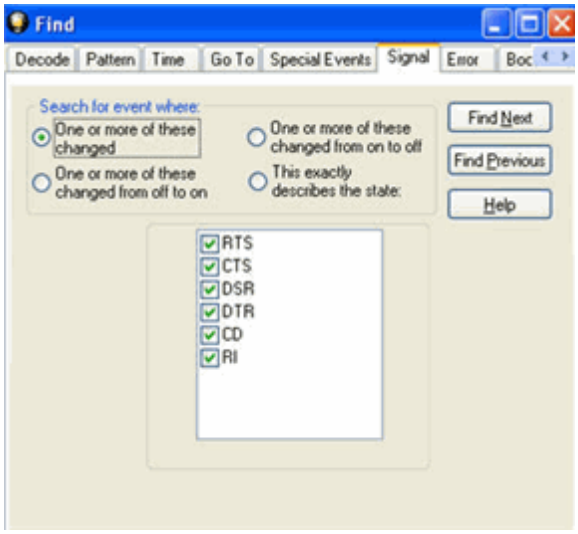
19.3 Searching for Control Signal Changes

Control signal searching allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where control signals changed.

To access the control signal search function

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to click the Find icon  from one of the toolbars
2. Click on the *Signal* tab of the Find dialog.



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

Selecting Control Signals to Search

The section with the check boxes allows you to specify which control signals the analyzer should pay attention to when doing the search. The analyzer pays attention to any control signal with a check mark.

- Click on a box to place a check mark next to a control signal
- Click again to uncheck the box
- By default, the analyzer searches all control signals, which means all boxes start out checked.

For example, if you are only interested in finding changes in RTS and CTS, you would check those two boxes and uncheck all the other boxes. This tells the analyzer to look only at the RTS and CTS lines when running the search. The other signals are ignored.

Searching for On, Off, or Changed States

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- One or more control signals changed
- One or more control signals changed from off to on
- One or more control signals changed from on to off

Searching for an event where one or more signals changed means that the analyzer looks at every control signal that you checked, and see if any one of those signals changed state at any time.

If you want to look at just one control signal:

- Check the box for the signal.
- Uncheck all the other boxes.
- Choose to search for an event where one or more signals changed.
- The analyzer notes the state of the selected signal at the point in the buffer where the cursor is, search the buffer, and stop when it finds an event where RTS changed state.
- If the end of the buffer is reached before an event is found, the analyzer tells you that no matches were found.

Searching for events where control signals changed state from off to on, or vice versa, is most useful if the signals are usually in one state, and you want to search for occasions where they changed state.

For example,

- If DTR is supposed to be on all the time but you suspect that DTR is being dropped
- Tell the analyzer to look only at DTR by checking the DTR box and unchecking the others
- Do a search for where one or more control signals changed from on to off.
- The analyzer would search the DTR signal and stop at the first event where DTR dropped from on to off.

Searching for an Exact State

To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.

- First, choose to search for an event where your choices exactly describe the state.
- This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each control signal.
- Choose which state you want each control signal to be in.

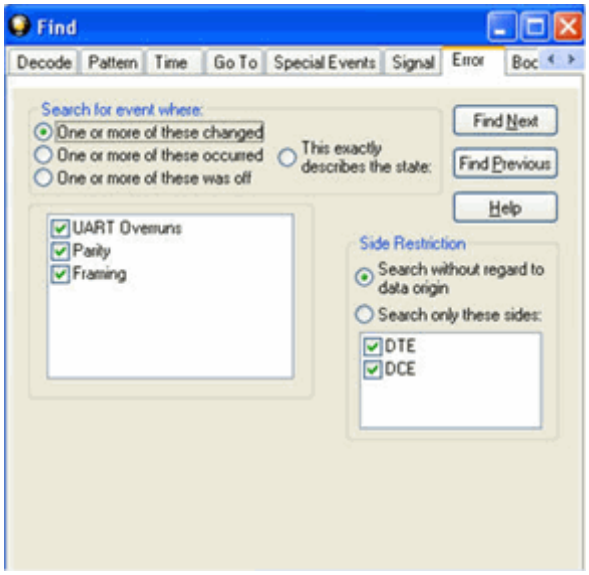
- Choose Don't Care to have the analyzer ignore the state of a control signal.
- When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.
- If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
- If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.

19.4 Searching for Data Errors

The analyzer can search for several types of data errors. You can choose which errors you want to search for and whether to search the DTE or DCE data or both. Bytes with errors are shown in red in the Event Display window, making it easy to find errors visually when looking through the data.

To access the data errors search function

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Error* tab of the Find dialog.



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

Selecting Which Errors to Search

The section with the check boxes allows you to choose which errors the analyzer should look for. Click on a box to check or un-check it

If you want to search only for overrun errors

- check the overrun box
- un-check the other boxes.

To search for all types of errors

- check all boxes

Searching for Error Conditions

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- one or more error conditions changed
  - one or more error conditions occurred
- one or more error conditions were off (i.e. no errors occurred)

The most common search is looking for a few scattered errors in otherwise clean data.

To do this type of search:

- choose to search for an event where one or more error conditions occurred
- choose which errors to look for
- By default, the analyzer looks for all types of errors.

In contrast, searching for an event where one or more error conditions were off means that the analyzer looks for an event where the errors were not present.

For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches the file, and finds the point at which framing errors stopped occurring.

Searching for an event where the error conditions changed means that the analyzer searches the data and stop at every point where the error condition changed from on to off, or off to on.

For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click Find Next, the analyzer stops at the point when the errors began occurring again.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where error conditions changed. The analyzer searches until it finds an event where error conditions changed or it reaches the end of the buffer, at which point the analyzer tells you that there are no more events found in the buffer. If you are searching for an exact match, the analyzer asks you if you want to continue searching from the beginning of the buffer.

Searching for Exact Error Conditions

To search for an exact state means that the analyzer finds events that exactly match the error conditions that you specify.

- Select the "This exactly describes the state" radio button.
- This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each error.
- On means that the error occurred
- Off means that the error did not occur
- Don't Care means that the analyzer ignores that error condition.
- Select the appropriate state for each type of error.

Example:

If you need to find an event where just an overrun error occurred, but not any other type of error, you would choose overrun error to be On, and set all other errors to Off. This causes the analyzer to look for an event where only an overrun error occurred.

If you want to look for events where overrun errors occurred, and other errors may have also occurred but it really doesn't matter if they did or not, choose overrun to be On, and set the others to Don't Care. The analyzer ignores any other type of error, and find events where overrun errors occurred.

To find the next error, click the Find Next button. To find an error that occurred earlier in the buffer to where you are, click the Find Previous button.

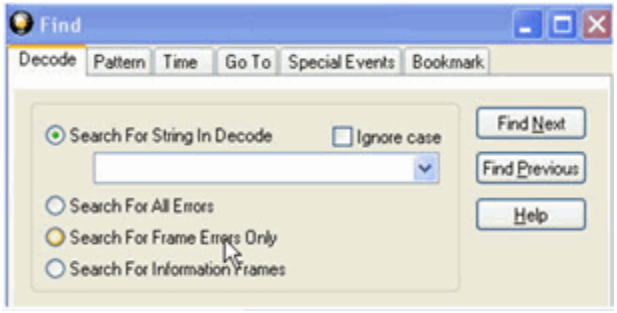
19.5Searching for Frame Errors

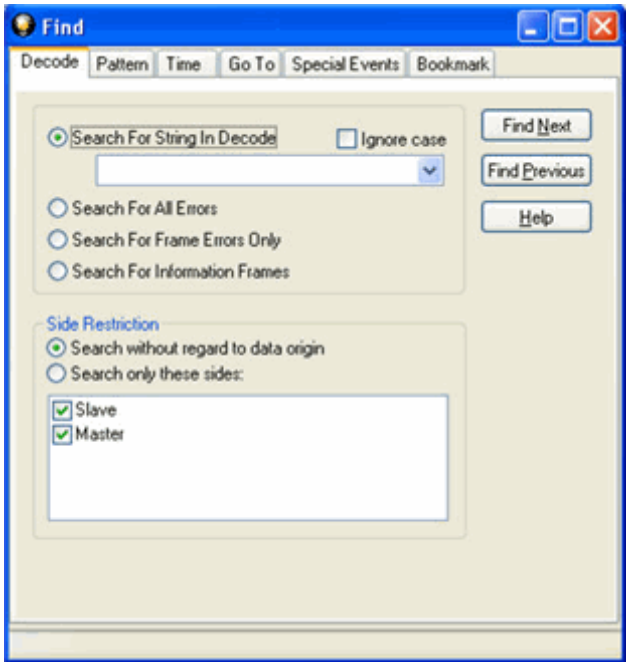
There are several options for error searching:

- Search for All Errors finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- Search for Frame Errors Only finds Frame specific errors, such as Frame Check errors.
- Search for Information Frame only searches Information Frames

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Decode* tab of the Find dialog.
3. Click the appropriate radio button for the type of search you want to perform or enter a value
4. Click Find Next.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

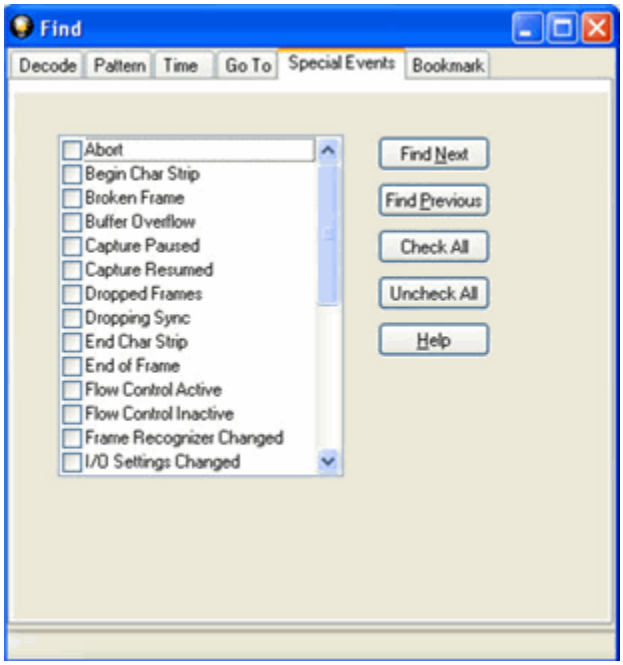
19.6Searching for Special Events

The analyzer inserts or marks events other than data bytes in the data stream.

For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker.

To access the search for special events function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars
2. Click on the *Special Events* tab of the Find dialog.



3. Check the event or events you want to look for in the list of special events.
4. Click Find Next.

Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

- Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of All Event Symbols.

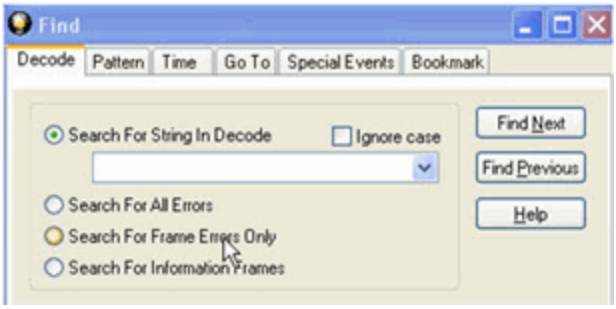
19.7 Searching within Decodes

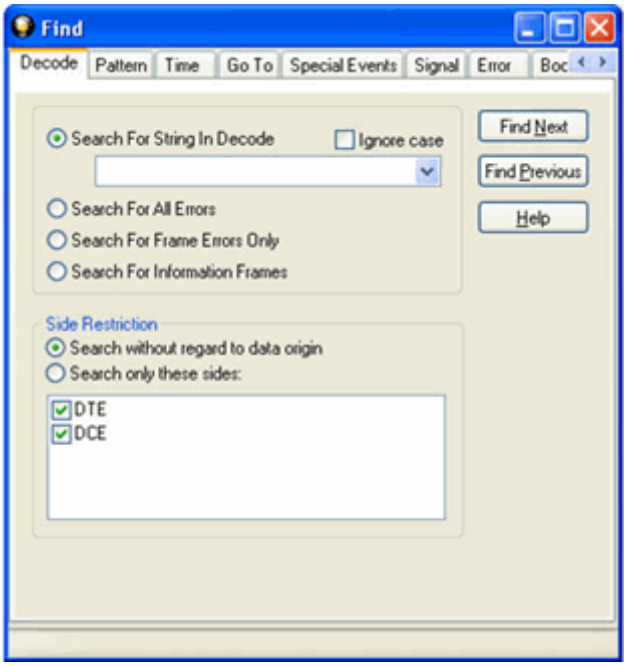
Searching within decodes lets you to do a string search on the data in the Decode Pane of the Frame Display window.

You can search one or both sides of the circuit, and your search can include wildcards. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string.

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars.
2. Click on the *Decode* tab of the Find dialog.





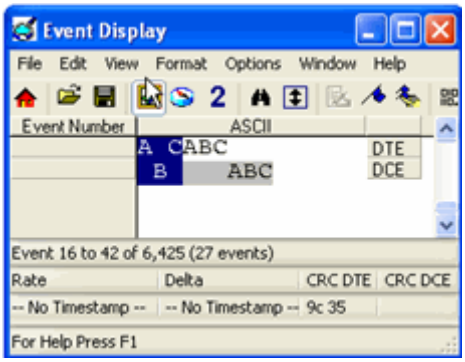
Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

19.8Side Restrictions

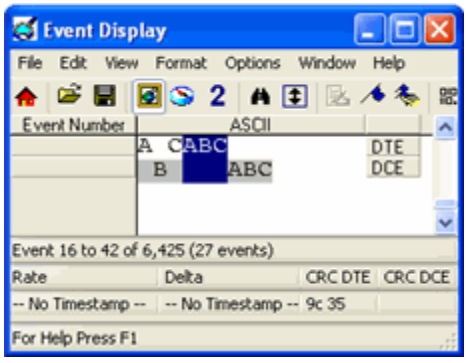
Side Restriction means that the analyzer looks for a pattern coming wholly from the DTE or DCE side. If you choose to search without regard for data origin, the analyzer looks for a pattern coming from one or both sides.

For example, if you choose to search for the pattern ABC and you choose to search without regard for data origin, the analyzer finds all three instances of ABC shown below.



The first pattern, with the A and the C coming from the DTE device and the B coming from the DCE is a good example of how using a side restriction differs from searching without regard to data origin. While searching without regard for data origin finds all three patterns, searching using a side restriction never finds the first pattern, because it does not come wholly from one side or the other.

If you choose to search for the pattern ABC, and you restrict the search to just the DTE side, the analyzer finds the following pattern:



In this example, the analyzer finds only the second pattern (highlighted above) because we restricted the search to just the DTE side. The first pattern doesn't qualify because it is split between the DTE and DCE sides, and the third pattern, though whole, comes from just the DCE side.

If we choose both the DTE and the DCE sides in the above example, then the analyzer finds the second pattern followed by the third pattern, but not the first pattern. This is because each side has one instance in which the whole pattern can be found. The analyzer completely searches the DTE side first, followed by the DCE side.

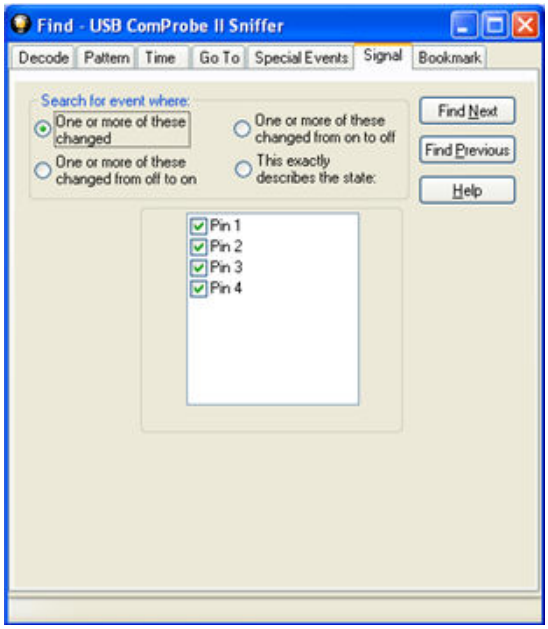
Side Restriction is available for pattern and error searching.

19.9 Searching by Signal

You can search using information originating from the Breakout Box.

1. Select one or more of the *checkboxes* for Pin 1, 2, 3, or 4.
   Click here to learn more about the Breakout Box and Pins 1 - 4.

2. Select one of the *four radio buttons* to choose the condition that must be met in the search



3. Click *Find Next* to locate the next occurrence of the search criteria or *Find Previous* to locate an earlier occurrence of the search criteria.

19.10 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

19.11 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

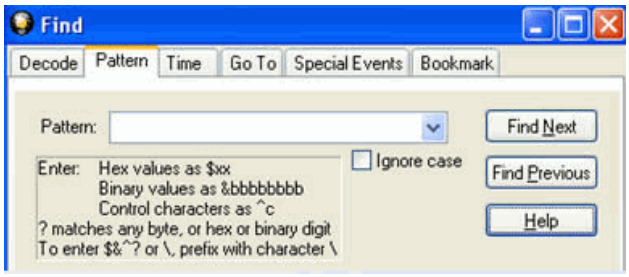
19.12 Entering Search Patterns (String Searches)

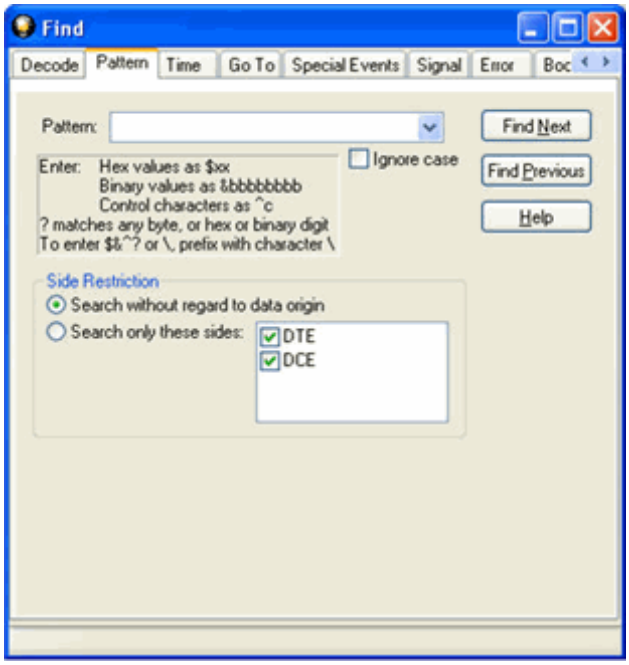
19.12.1 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards. You can search one or both sides of a circuit containing interwoven data such as serial communication.

To access the search by pattern function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon  from one of the toolbars.
2. Click on the *Pattern* tab of the Find dialog.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

19.12.2 Entering Characters

Various characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are used as prefixes to let you to enter hex, binary, control or wildcard characters.

1. Place the cursor in the Pattern box and type in your string.
2. Click Find Next in order to find the next occurrence of the string.
3. Click on Find Next as many times as necessary until the analyzer has searched all the data.
4. Clicking on Find Previous searches the buffer backwards.

The escape character is the backslash \. Use this character when you want to search for one of the above restricted characters. For example, to search for a $, you enter \$. To search for a \, enter \\.

Check Ignore Case to do a case-insensitive search.

19.12.3 Entering Hex or Binary

Hex or Binary values are used when creating a search string on the Find dialog.

To enter a hex value :

1. Enter a $ followed by two hex digits.
2. For example, to search for hex 00 01, enter $00$01.
3. If you need to specify the $ as a character, use \$.
4. The $ symbol tells the analyzer that the following characters are hex digits

To enter a binary value:

- The & symbol tells the analyzer that a binary number comes next. For example, to search for binary 00001111, you would use &00001111.
- If you need to specify the & as a character, use \&.

19.12.4 Control Characters

Various control characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are unavailable. The ^ (caret) is used to enter the control characters Ctrl-A through Ctrl-Z and Ctrl-@,[,\,],- when using the ASCII character set. For example, ^A specifies Ctrl-A ($01) and ^@ specifies ASCII NUL ($00).

If you need to specify the ^ as a character, use \^.

Note that neither the ^ character nor control characters exist in Baudot, so attempts to search for the ^ character results in an error message. The ^ character exists in EBCDIC, but control characters do not. A search for ^A in EBCDIC matches any occurrence of ^A ($5F$C1). You do not need to use the escape character to search for a ^ character in EBCDIC.

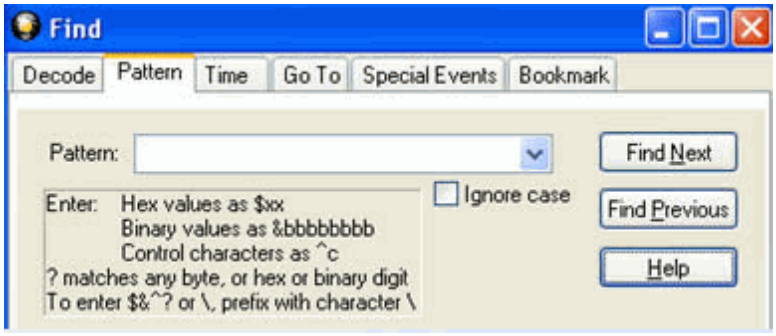
19.12.5 Wildcard Character

A wildcard can be used when creating a search string on the Find dialog.

The wildcard character is the question mark (?). The analyzer supports wildcard searching at the byte, nibble and bit level. Wildcards can be used in place of characters, hex digits, and binary digits. If you need to search for a ?, you can use \?.

19.12.6 Examples of Search Strings

In the Find function on the Frame Display, Event Display, or Protocol Navigator, you can search for any single byte in the range of hex $10 through $1F, type $1?.



&111111?? searches for binary numbers beginning with 111111 and ending with any combination of 1 and 0. 11111100, 11111101, 11111110, and 11111111 are all strings that match the search criteria.

To search for any four character string which starts with an L and ends with an ES, type L?ES.

You can combine formats in one string. For example, another way to specify a search for the string L?ES is $4C&????????&01000101S.

19.13 Searching by Time

19.13.1 Searching by Time

The analyzer can search by time in two different ways.

- **Absolute**

  An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.

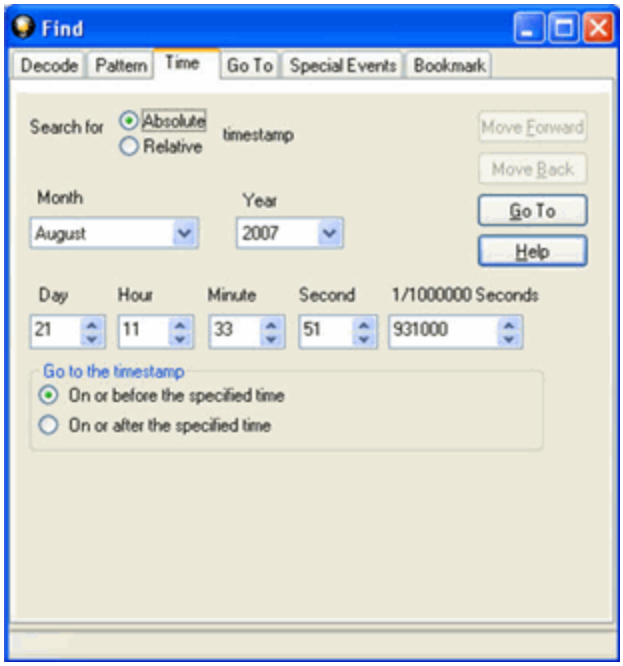
- **Relative**

  A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

Note that the analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon  from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.
3. Use the "Search for" radio buttons at the top of the dialog to indicate the search type



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

19.13.2 Searching with Absolute Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may also select the Find icon  from one of the toolbars
2. Click on the *Time* tab of the Find dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

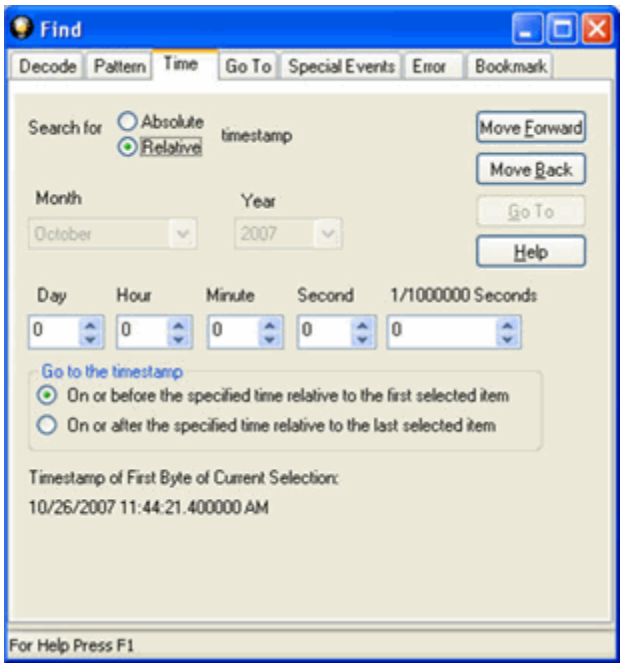
3. Specify the time to search for by using the counters in the middle of the window.
   - Click on the arrows next to each item to increase or decrease the value of each counter.
   - By default, the counters display the timestamp of the first event in the file
4. After selecting the time, click on the Go To button to start the search.

Sometimes there can be more than one event with the same timestamp. The system highlights all events with the specified timestamp.

19.13.3 Searching with Relative Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also select the Find icon  from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

3. Click on the event in the Event Display window that you want to begin the search from. The event must have a timestamp in order for relative timestamp search to work.

4. In the *Find* dialog, use the counters in the middle of the window to specify the time interval you want to jump.
   You can specify intervals in days, hours, minutes, seconds, and fractions of a second, or any combination of these.

5. When you have specified the time interval you want to use, click on the Move Forward or Move Backward buttons to start the search from the current event.

For example, to search for an event occurring 10 seconds after the currently selected event, choose to do a relative timestamp search, use 10 seconds for your time interval, and click on Move Forward.

As with absolute timestamping, the analyzer highlights all events with the specified timestamp.

19.13.4 Choosing "On or Before" or "On or After"

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the "Go to the timestamp" box.

If you are searching forward in the buffer, you usually want to choose the "On or After" button. If you choose the "On or Before" option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

20 Bookmarks

20.1 Bookmarks

- Bookmarks are a way to mark frames or events in a capture file. You can search for bookmarks and move quickly between bookmarks.
- Bookmarks appear as a magenta triangle next to the frame number in the Frame Display window. Any comment associated with the bookmark appears in the Bookmark column.
- When you add or change a bookmark, you are asked if you want to save your changes when you close the capture file, and given the option of saving the bookmarks to the current file or to a new one. See Confirming CFA Changes for more information.

20.2 Adding, Modifying or Deleting a Bookmark

You can Add, Modify, or Delete a Bookmark from the Add Bookmark dialog from the Frame Display, Event Display, or the Protocol Navigator.

Add:

1. Select the frame or event you want to bookmark.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. Or simply select the *Add or Modify Bookmark*  icon on one of the toolbars.
3. In the dialog box, add a comment if you wish.
4. Click *OK*.

You can also add a bookmark by right-clicking on the frame and choosing Add Bookmark from the right-click menu.

Modify and Delete:

1. Select the frame or event with the bookmark to be edited.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display  , Event Display  , or the Protocol Navigator  . Or simply select the *Add or Modify Bookmark*  icon on one of the toolbars.

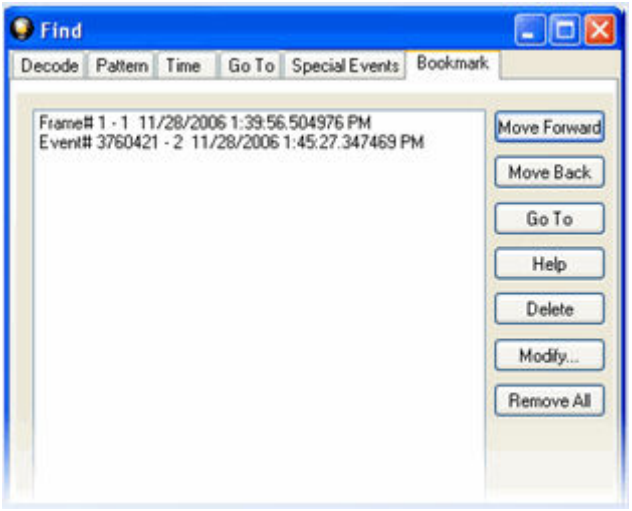
3. To modify a bookmark, change the comment in the dialog box and click OK.
4. To delete a bookmark, click the Delete button.

You can also modify or delete a bookmark by right-clicking on the frame and choosing Modify Bookmark from the right-click menu.

20.3 Displaying All and Moving Between Bookmarks

There are two ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Click the Display All Bookmarks icon  . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.



- To delete a bookmark, select it and click the Delete button.
- To modify a bookmark, select it and click the Modify button.
- Click Remove All to delete all the bookmarks.

21 Filtering

21.1 Difference Between Ethernet Capture Filters and Display Filters

There are two types of filters: Display filters and Ethernet capture filters.

An *Ethernet capture filter* looks at frames when they are first captured. If the frame satisfies the filter criteria, the frame is kept and put in the capture buffer. If the frame does not satisfy the filter criteria, it is thrown away. Data that is filtered out using an Ethernet capture filter cannot be recovered. Only one Ethernet capture filter can be active at a time. Capture filtering is not available in serial products yet.

A *display filter* looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Unlike an Ethernet capture filter, where data that does not match is thrown away, all the data is kept when using a display filter. The filter just displays a subset of the data. Multiple display filters can be used simultaneously, and different windows can be displaying data using different filters.

21.2 Display Filters

21.2.1 About Display Filters

Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filters

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.

- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog or through filter selection on the Protocol Navigator.

21.2.2 Including and Excluding Radio Buttons

All filter dialog boxes contain an "Include" and an "Exclude" radio button. These buttons are mutually exclusive. The "Include/Exclude" selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

Include:

A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

Exclude:

A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

21.2.3 Creating a Display Filter

There are two steps to using a display filter. Define the filter conditions, and then apply the filter to the data set. The system combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator*  or the *Frame Display*  window or select *Apply/Modify Display Filters* from the *Filter* menu to open the *Set Condition* dialog box.
2. Select Include or Exclude to
3. Select the initial condition for the filter from the drop-down list.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.
5. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click OK. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The *Set*

Condition dialog box closes, creates a tab on the *Frame Display* with the filter name, and applies the filter.

The filter appears in the Quick Filtering and Hiding Protocols dialog also.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Notes:

The system requires naming and saving of all filters created by the user.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

21.2.4 Named Display Filters

You can create a unique display filter by selecting a data type on the Frame Display and using a right click menu. When you create a Name Filter, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the Frame Display panes.

1. Select a frame in the Frame Display Summary Pane.
2. Right click in the one of the data columns in the Summary Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select Filter in (data type)

The Filtering Results dialog appears.

4. Enter a name for the filter
5. Select OK.

The filter you just created appears in the Named Filters section of the Quick Filtering dialog.

21.2.5 Using Compound Display Filters

Compound filters use Boolean logic to create complex and precise filters. There are three primary Boolean logic operators: AND, OR, and NOT.

The AND operator narrows the filter, the OR operator broadens the filter, and the NOT operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Click the *Advanced* button on the *Set Condition* dialog box.
3. Select the initial condition for the filter from the combo box.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.
5. Click the Plus icon  on the left side of the dialog box and repeat steps 3 and 4 for the next condition. Continue adding conditions until your filter is complete.
6. Include parentheses as needed and set the Boolean operators.
7. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click *OK*. The *Set Condition* dialog box closes, creates a tab on the Frame Display with the filter name, and applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the Protocol Navigator and the Frame Display windows.

Note:

Use the *Up*  and *Down*  arrow icons on the left side of the dialog box to order your conditions, and the *Delete* button  to delete conditions from your filter.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

21.2.6 Defining Node and Conversation Filters

There are two steps to using Node and Conversation display filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Choose "frames with the conversation" as the initial condition from the *Select* combo box.

3. Select an address type from the *Type* combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first *Address* combo box.
5. Choose a direction arrow from the *Direction* box. The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.
6. If you want to filter on just one node address, skip step 7 & 8, and continue with step 9.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select an address type for the second node address from the *Type* combo box.
8. Select a node address from the second *Address* combo box.
9. Click *OK*. The *Set Condition* dialog box closes and the analyzer applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Note:

The *OK* button is unavailable (grayed out) until the condition selections are complete.

21.2.7 Using Advanced Display Filtering Techniques

Intermediate to advanced users, with a solid knowledge of filter definition and application may find it useful to create some of the more common filters "on the fly" using the advanced filtering techniques.

Choose one of the panes in either the *Frame Display* or *Protocol Navigator* windows:

1. Place the cursor over a parameter you wish to filter on such as a node address or protocol type, and right click.
2. A pop up menu appears with selections for filtering.
3. Select the filter.
4. The system either closes the menu and applies the filter, or displays the *Set Conditions* dialog box with the known parameters filled in and the additional options available to complete the conditions statement.

21.2.8 Deleting and Hiding Display Filters

21.2.8.1 The Difference Between Deleting and Hiding Display Filters

If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the *Set Conditions* dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

21.2.8.2 Deleting Saved Display Filters

1. Select *Delete Display Filters* from the *Filter* menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Delete Named Condition* dialog. The system displays the *Delete Named Condition* dialog with a list of all user defined filters.
2. Select the filter to be deleted from the drop-down list.
3. Click the *Delete* button.
4. Click *OK*. The *Delete Named Condition* dialog box closes and the system deletes the filter.

Hiding/Revealing a Display Filter

1. Select "Hide/Show Display Filters" from the filter menu on either the *Protocol Navigator*  or the *Frame Display*  window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the *Hide* button.
4. Click *OK*. The *Hide/Show* dialog box closes, and the system hides the filter and removes the filter tab from the *Frame Display*.

Revealing a Hidden Display Filter

There are several ways to reveal a hidden filter. One can open the *Quick Filter* dialog and check the box next to the hidden filter, or check the box next the hidden filter in the *Protocol Navigator* display.

Perform the following actions to reveal a hidden filter:

1. Select "Hide/Show Display Filters" from the filter menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the *Show* button.
4. Click *OK*. The *Hide/Show* dialog box closes and the system reveals the filter and adds the filter tab to the *Frame Display*.

Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the

Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

21.2.9 Editing Filters

21.2.9.1 Modifying a Condition in a Filter

1. Click the *Display Filters* icon  on either the *Protocol Navigator*  or the *Frame Display*  window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Edit the desired parameter of the condition.
   Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

21.2.9.2 Deleting a Condition in a Filter

1. Click the *Display Filters* icon  on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Select the desired condition from the filter definition.
3. Click the Delete icon.
4. Edit the Boolean operators and parentheses as needed.
5. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

21.2.9.3 Renaming a Display Filter

1. Select "Rename Display Filters" from the *Filter* menu in either the *Protocol Navigator*  or the *Frame Display*  window to open the *Rename Filter* dialog. The system displays the *Rename Filter* dialog with a list of all user defined filters.
2. Select the filter to be renamed from the combo box.
3. Enter a new name for the filter in the text box.
4. Click *OK*. The *Rename Filter* dialog box closes and the system renames the filter.

21.3 Ethernet Capture Filters

21.3.1 Creating and Using an Ethernet Capture Filter

There are two steps to using an Ethernet capture filter. Define the filter conditions, and then apply the filter to the steaming data. FTS combines both filter definition and application in one dialog.

1. Select "I/O Settings" from the *Options* menu.
2. Click the *Define Conditions* tab.
3. FTS supports four different types of filters. Click on the links below for more information about defining each type of filter.
   BPF (Create a custom filter)
   Node (Includes filtering on a Ethernet single node as well as conversations between nodes)
   Pattern
   Predefined (Includes protocols and protocol specific filters)
4. After you define the filter, click the *Capture Filters* tab.
5. Choose the filter or filters to apply. See Applying An Ethernet Capture Filter.
6. Click *OK*. The filters dialog closes and FTS applies the filter.

Note:

Ethernet Capture filtering is not available when viewing a capture file. Ethernet Capture filters look at frames as they are being captured and either discards them or puts them in the buffer based on the filter criteria. Display filters look at the frames in the buffer and display only those frames that match the criteria.

21.3.2 Applying an Ethernet Capture Filter

Note:Ethernet Capture filters are unavailable when viewing a capture file.

1. Select "I/O Settings" from the *Options* menu to display the capture filter dialog.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to include in the filter.
4. The *Filter Representation* box at the bottom of the dialog displays text describing the filter. Click the checkbox to see the tcpdump syntax.
5. If you make a mistake and want to start over, click the Reset button.
6. [Optional] Type a name in the Compound Filters box at the top of the dialog and click the *Save Compound Filter* icon. In the future, you will be able to select the same condition(s) by selecting the name from the box.
7. Click *OK* (at the bottom of the far left side of the dialog). The filters dialog closes and FTS applies the capture filter.

When using an Ethernet capture filter, the *Control* window displays text describing the capture filter conditions to the right of the toolbar, and the *Control* window status bar displays "Run-Filter" as the "Capture Status".

Ethernet Capture filters look at data as it is being captured, and stores only those frames that match the filter criteria in the buffer.

21.3.3 Removing an Ethernet Capture Filter

Removing an Ethernet capture filter can be done by following the steps below :

1. To remove an Ethernet capture filter, select "I/O Settings" from the *Options* menu to display the filters dialog.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. FTS displays the Ethernet capture filter currently in use in the *Conditions Selected in Filter* box. Click the condition(s) you want to remove. Use the arrow buttons to move the conditions to the box on the left, OR click the double arrow button to remove all conditions.
4. Click *OK* (at the bottom of the far left side of the dialog). The Filters dialog closes and FTS removes the filter.

21.3.4 Defining Node and Conversation Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the word *Node*. The right side of the dialog changes to display the Node definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the center top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. In the *Node A* section, select the radio button for the type of address you want. All means to pass all frames. Type the MAC or IP address of the node you wish to filter on.
6. Choose a direction arrow from the Direction box. The left arrow filters on all frames where Node A is the destination, the right arrow filters on all frames where Node A is the source, and the double arrow filters on all frames where Node A is either the source or the destination.
7. If you want to filter on just one node, stop right here. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.
8. If you want to filter on traffic going between two nodes (i.e. a conversation), select an address type and add the MAC or IP address of the second node in the Node B box. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

21.3.5 Selecting Predefined Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. In the tree view on the left, click the plus sign next to the word Predefined to expand that section.
4. Click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to include in the filter.
5. Click *OK*. The filter dialog closes and FTS applies the filter.

Predefined filters are not editable. FTS supplies many predefined filters applicable to the protocols available. This section shows the available predefined filters.

21.3.6 Defining Pattern or Offset Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the word *Pattern*. The right side of the dialog changes to display the Pattern definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. Enter a pattern in the *Look for this Pattern* box. Use $ to specify a hex byte (e.g. $00 looks for a null character).
6. Enter the offset and where the offset should start in the *Offset this many bytes:* and *From start of:* boxes. FTS can begin counting from the start of the frame or the start of a protocol header. An offset of 0 means to look at the first byte, an offset of 1 means to look at the second byte, etc.
7. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

21.3.7 Using BPF to Create a Custom Ethernet Capture Filter

You can create, modify, and delete filters using the I/O menu items on the Protocol Navigator and Frame Display dialogs.

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the word *BPF*. The right side of the dialog changes to display the BPF definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. Enter the BPF string in the *Expression* box (See Berkeley Packet Filtering Man Page).
6. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

Filtering functionality is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. The Filter String Formats help topic describes how to write a filter string for the most common types of filters. For the full description of BPF syntax, click here for the instructions from the tcpdump man page.

21.3.8 Creating/Deleting a Compound Filter

A compound filter is a set of conditions grouped together to create a more complex filter which can then be named as a separate filter.

It's a convenient way of grouping conditions into one filter set and remembering what the filter does. Compound filters can be selected from a list on the *Capture Filters* tab, making it very easy to reuse groups of conditions.

To create a compound filter:

1. Move the conditions to the Select Filters to Apply box
2. Click the Save Compound Filter button.
3. Give the filter a name.

To delete a compound filter:

1. Select the filter from the list box
2. Click the *Delete Filter* button. This deletes the filter only. It does not delete the conditions used in the filter.

Compound filters also appear in the Named Filters box on the Protocol Navigator window. This lets you quickly apply the filter from the Protocol Navigator without having to open the Filters dialog.

21.3.9 Naming Ethernet Capture Filters

You can name any condition to something more meaningful to you. For example, you can name Node filters of IP addresses to show the name of the device corresponding to that address.

To name a filter:

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. Define the filter in the BPF, Node or Pattern sections of the *Define Conditions* tab.
4. Add a name in the *Name* box.
5. When you click the *Add* button, the name displays in the tree in the left pane.

Named filters also appear in the *Named Filters* box on the Protocol Navigator window. This lets you quickly apply the filter from the *Protocol Navigator* without opening the filters window.

21.3.10 Modifying a Condition in an Ethernet Capture Filter

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to modify. The right side of the dialog changes to display the definition pane for the type of condition selected and places the contents of the condition in the pane.
4. Change the condition to the desired state.
5. Click the Modify button at the bottom of the definition pane, and click the *OK* button at the bottom of the dialog.

21.3.11 Deleting a Condition in an Ethernet Capture Filter

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to delete. The right side of the dialog changes to display the definition pane for the type of condition selected, and put the contents of the condition in the pane.
4. Click the *Delete* button at the bottom of the definition pane, and click the *OK* button at the bottom of the dialog.

21.3.12 Filter Formats

21.3.12.1 Filter String Formats

Filtering functionality in the analyzer is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. Because BPF was designed to filter Ethernet data, there are some limitations when filtering other types of data. For the full description of BPF syntax, click here for an excerpt from the tcpdump man page.

The filter format consists of one or more "qualifiers", which may or may not be followed by an ID, which identifies the thing to be filtered on.

Qualifiers

There are three kinds of qualifiers: type, direction and protocol.

- *Type qualifiers* tell you what kind of thing the ID refers to. There are three possible types: host, net and port. If no type is given, host is assumed.

- *Direction qualifiers* specify the direction of traffic to or from the ID. There are four possible directions:
    - src - source. Filters on frames for which the ID is the source.
    - dst - destination. Filters on frames for which the ID is the destination.
    - src or dst - source or destination. Filters on frames for which the ID is either the source or the destination.
    - src and dst - source and destination. Filters on frames for which the ID is both the source and the destination

  If no direction is given, src or dst is assumed.
- *Protocol qualifiers* specify a particular protocol. Possible protocol qualifiers are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. If no protocol is given, all protocols consistent with the type are assumed.

IDs, or Identifiers

Identifiers are usually a name or a number identifying a particular node, protocol, network, etc. Examples are Ethernet MAC addresses or IP addresses. To specify a hex value, use 0x before the value. Example: 0x50.

Expressions and Relational Operators

You can combine identifiers using the following:

- 'and' or '&&' - concatenation. Filters on frames where both identifiers are true.
- 'or' or '||' - alternation. Filters on frames where one or both of the identifiers is true.
- 'not' or '!' - negation. Excludes a frame if the identifier is true.
- Negation has highest precedence and is evaluated first. Alternation and concatenation have equal precedence and are evaluated left to right.
- Use parentheses to combine expressions. Example: to filter on all frames from Abel and either Baker or Charlie, use: host Abel and (Baker or Charlie)

Filter on MAC Address

To filter on all frames to and from an Ethernet MAC Address, use the following syntax:

ether host 00:01:02:03:04:05

To filter on all frames to and from two MAC Addresses:

ether host 00:01:02:03:04:05 and 06:07:08:09:0a:0b

Filter on IP Address

To filter on all frames to and from an IP address, use the following syntax:

ip host 100.200.300.4

To filter on all frames to and from two IP addresses, use:

ip host 100.200.300.4 and 100.200.300.5

Filter on Protocol

To filter on a protocol, enter the protocol name in the string box. Possible protocols are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. You can also filter on protocols within protocols using the proto keyword.

Examples:

- ip - filters on all IP frames
- ip proto \tcp - filters on all TCP frames (tcp is a keyword and must be escaped using the '\' when used as an ID)
- port 80 - filters on all frames 'to and from' a TCP port, in this case port 80 (HTTP)

Filter at an Offset

To specify an offset from a protocol, place the value in brackets.

ether[13]>5 - examines the 13th byte from Ethernet start of frame for a value greater than 5 (remember that the first byte is at offset zero).

21.3.12.2 Berkeley Packet Filtering Main Page

The following text is taken from the tcpdump main page. References to CShell have been removed, along with some references to escape characters which are relevant only when running tcpdump under CShell and which are not relevant to filtering in FTS.

Expression selects which packets are dumped. If no *expression* is given, all packets on the net are dumped. Otherwise, only packets for which *expression* is `true' are be dumped. The *expression* consists of one or more *primitives*. Primitives usually consist of an *id* (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

type	qualifiers say what kind of thing the id name or number refers to. Possible types are **host**, **net** and **port**. E.g., `host foo', `net 128.3', `port 20'. If there is no type qualifier, **host** is assumed.
dir	qualifiers specify a particular transfer direction to and/or from id. Possible directions are **src**, **dst**, **src** or **dst** and **src** and **dst**. E.g., `src foo', `dst net 128.3', `**src** or **dst** port ftp-data'. If there is no dir qualifier, src or dst is assumed. For `null' link layers (i.e. point to point protocols such as slip) the **inbound** and **outbound** qualifiers can be used to specify a desired direction.
proto	qualifiers restrict the match to a particular protocol. Possible protos are: **ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp** and **udp**. E.g., `ether src foo', `arp net 128.3', `tcp port 21'. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., `src foo' means `(ip or arp or rarp) src foo' (except the latter is not legal syn- tax), `net bar' means `(ip or arp or rarp) net bar' and `port 53' means `(tcp or udp) port 53'. [`fddi' is actually an alias for `ether'; the parser treats them identically as meaning ``the data link level used on the specified network interface.'' FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just

as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression.]

In addition to the above, there are some special `primitive' keywords that don't follow the pattern: **gateway, broadcast, less, greater** and **arithmetic** expressions. All of these are described below.

More complex filter expressions are built up by using the words **and**, **or** and **not** to combine primitives. E.g., `host foo and not port ftp and not port ftp-data'. To save typing, identical qualifier lists can be omitted. E.g., `tcp dst port ftp or ftp-data or domain' is exactly the same as `tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain'. Allowable primitives are:

dst host *host*	True if the IP destination field of the packet is *host*, which may be either an address or a name.
src host *host*	True if the IP source field of the packet is *host*.
host *host*	True if either the IP source or destination of the packet is *host*. Any of the above host expressions can be prepended with the keywords, **ip**, **arp**, or **rarp** as in: **ip host** *host* which is equivalent to: **ether proto** *ip* and **host** *host* If *host* is a name with multiple IP addresses, each address is checked for a match.
ether dst *ehost*	True if the ethernet destination address is *ehost*. *Ehost* may be either a name from /etc/ethers or a number for numeric format.
ether src *ehost*	True if the ethernet source address is *ehost*.
ether host *ehost*	True if either the ethernet source or destination address is *ehost*.
gateway *host*	True if the packet used *host* as a gateway. I.e., the ethernet source or destination address was *host* but neither the IP source nor the IP destination was *host*. *Host* must be a name and must be found in both /etc/hosts and /etc/ethers. (An equivalent expression is **ether host** *ehost* and **not host** *host* which can be used with either names or numbers for *host* / *ehost*.)
dst net *net*	True if the IP destination address of the packet has a network number of *net*. *Net* may be either a name from /etc/networks or a network number for details).
src net *net*	True if the IP source address of the packet has a network number of *net*.
net *net*	True if either the IP source or destination address of the packet has a network number of *net*.
net *net* **mask**	True if the IP address matches *net* with the specific netmask. May be

mask	qualified with **src** or **dst**.
net *net/len*	True if the IP address matches *net* a netmask *len* bits wide. May be qualified with **src** or **dst**.
dst port *port*	True if the packet is ip/tcp or ip/udp and has a destination port value of *port*. The *port* can be a number or a name used in /etc/services. If a name is used, both the port number and protocol are checked. If a number or ambiguous name is used, only the port number is checked (e.g., **dst port 513** prints both tcp/login traffic and udp/who traffic, and **port domain** prints both tcp/domain and udp/domain traffic).
src port *port*	True if the packet has a source port value of *port*.
port *port*	True if either the source or destination port of the packet is *port*. Any of the above port expressions can be prepended with the keywords, **tcp** or **udp**, as in: **tcp src port** *port* which matches only tcp packets whose source port is *port*.
less *length*	True if the packet has a length less than or equal to *length*. This is equivalent to: **len <=** *length*.
greater *length*	True if the packet has a length greater than or equal to *length*. This is equivalent to: **len >=** *length*.
ip proto *protocol*	True if the packet is an ip packet of protocol type *protocol*. *Protocol* can be a number or one of the names *icmp*, *igrp*, *udp*, *nd*, or *tcp*. Note that the identifiers *tcp*, *udp*, and *icmp* are also keywords and must be escaped via backslash (\).
ether broadcast	True if the packet is an ethernet broadcast packet. The *ether* keyword is optional.
ip broadcast	True if the packet is an IP broadcast packet. It checks for both the all-zeroes and all-ones broadcast conventions, and looks up the local subnet mask.
ether multicast	True if the packet is an ethernet multicast packet. The *ether* keyword is optional. This is shorthand for `**ether[0] & 1 != 0**'.
ip multicast	True if the packet is an IP multicast packet.
ether proto *protocol*	True if the packet is of ether type *protocol*. *Protocol* can be a number or a name like *ip*, *arp*, or *rarp*. Note these identifiers are also keywords and must be escaped via backslash (\). [In the case of FDDI (e.g., `**fddi protocol arp**'), the protocol identification comes from the 802.2 Logical Link Control (LLC) header, which is usually layered on top of the FDDI header. *Tcpdump* assumes, when filtering on the protocol identifier, that all FDDI packets include an LLC header, and that the LLC header is in so-called SNAP format.]
decnet	True if the DECNET source address is *host*, which may be an address of the

src *host*	form ``10.123'', or a DECNET host name. [DECNET host name support is only available on Ultrix systems that are configured to run DECNET.]
decnet dst *host*	True if the DECNET destination address is *host*.
decnet host *host*	True if either the DECNET source or destination address is *host*.
ip, arp, rarp, decnet	Abbreviations for: **ether proto** *p* where *p* is one of the above protocols.
lat, moprc, mopdl	Abbreviations for: **ether proto** where *p* is one of the above protocols. Note that *tcpdump* does not currently know how to parse these protocols.
tcp, udp, icmp	Abbreviations for: **ip proto** *p* where *p* is one of the above protocols.
expr relop expr	True if the relation holds, where *relop* is one of >, <, >=, <=, =, !=, and *expr* is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+, -, *, /, &, |], a length operator, and special packet data accessors. To access data inside the packet, use the following syntax: *proto* [*expr* : *size*] *Proto* is one of **ether**, **fddi**, **ip**, **arp**, **rarp**, **tcp**, **udp**, or **icmp**, and indicates the protocol layer for the index operation. The byte offset, relative to the indicated protocol layer, is given by *expr*. *Size* is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword **len**, gives the length of the packet. For example, `**ether[0] & 1 != 0**' catches all multicast traffic. The expression `**ip[0] & 0xf != 5**' catches all IP packets with options. The expression `**ip[6:2] & 0x1fff = 0**' catches only unfragmented datagrams and frag zero of fragmented datagrams. This check is implicitly applied to the **tcp** and **udp** index operations. For instance, **tcp[0]** always means the first byte of the TCP *header*, and never means the first byte of an intervening fragment. Primitives may be combined using a parenthesized group of primitives and operators.

Negation (`**!**' or `**not**').

Concatenation (`**&&**' or `**and**').

Alternation (`||' or `**or**').

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right.

Note that explicit **and** tokens, not juxtaposition, are now required for concatenation. If an identifier is given without a keyword, the most recent keyword is assumed. For example,

not host vs and ace is short for **not host vs and host ace** which should not be confused with **not (host vs or ace)**.

EXAMPLES

To print all packets arriving at or departing from sundown:

host sundown

To print traffic between helios and either hot or ace:

host helios and (hot or ace)

To print all IP packets between ace and any host except helios:

ip host ace and not helios

To print all traffic between local hosts and hosts at Berkeley:

net ucb-ether

To print all ftp traffic through internet gateway snup:

gateway snup and (port ftp or ftp-data)

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).

ip and not net localnet

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

tcp[13] & 3 != 0 and not src and dst net localnet

To print IP packets longer than 576 bytes sent through gateway snup:

gateway snup and ip[2:2] > 576

To print IP broadcast or multicast packets that were not sent via ethernet broadcast or multicast:

ether[0] & 1 = 0 and ip[16] >= 224

To print all ICMP packets that are not echo requests/replies (i.e., not ping packets):

icmp[0] != 8 and icmp[0] != 0

AUTHORS

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. Full Copyright notice.

21.3.13 Saving and Loading Capture Filter Files

21.3.13.1 Saving Ethernet Capture Filters to a File

From the Frame Display or Protocol Navigator windows:

1. Select "I/O Settings" from the *Options* menu to display the filters dialog.

2. Click on the *Define Conditions* tab at the top of the window.
3. Define one or more conditions.
4. Enter a name for the filter in the *Name*: field.
5. Click OK.

Saving a filter file saves the conditions you've created. You can combine these conditions in multiple ways to create different Ethernet capture filters.

If you create a condition set (a group of conditions to apply all at the same time) for an Ethernet capture filter and want to save the condition set, name the filter, and then save the filter file. The named filter is saved as part of the filter file, and is available the next time the file is opened.

21.3.13.2 Opening an Ethernet Capture Filter File

From the Frame Display or Protocol Navigator windows:

1. Select "I/O Settings" from the *Options* menu to display the filters dialog.
2. Select *File >Open* icon and browse to the filter file.

Filter files have a .filter extension by default. The default location for filter files is the **My Configurations** directory. However, the user may choose to set another default location using the Changing Default File Locations procedure.

3. Open the file.

21.4 Protocol Filtering from the Frame Display

21.4.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

21.4.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

21.4.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.

2. On the *Frame Display* window, click the starred *Quick Filtering* icon  or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

3. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.

4. Then click *OK*.

21.4.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display*  window.
2. Click the starred *Quick Filter* icon  or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

21.5 Protocol Filtering from the Protocol Navigator

21.5.1 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

21.5.2 Filtering on all Frames with Bookmarks

To filter on all frames with bookmarks:

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Bookmarks* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

21.5.3 Filtering on all Frames with Errors from the Protocol Navigator

To filter on all frames with errors :

1. Open the *Protocol Navigator*  window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

21.5.4 Filtering on all Frames with Special Information Nodes

To filter on all frames with special information nodes:

1. Open the Protocol Navigator  window.
2. Check the All Special Information Nodes box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

21.5.5 Named Filters

You can create, modify, and delete filters using the Filter menu items on the Protocol Navigator and Frame Display dialogs.

If you create a *Named* filter using the *Filters* dialog, the filter appears in the *Named Frame Filters* pane in the bottom left corner of the *Protocol Navigator* window.

1. Check the boxes next to the names of the filters you want to use.

Note that using a named filter affects the contents of the *Frame Display* window as well.

22 Saving Data

22.1 Saving Your Data

You can save all or part of a capture file. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

On the Control toolbar you can set up to capture a single file or series of files. Click here to see those settings.

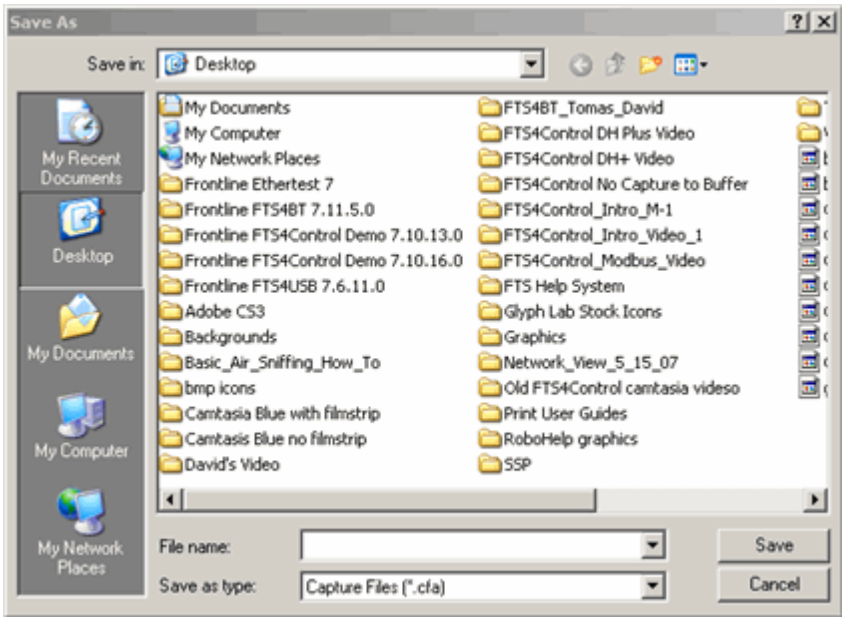
There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data.

22.2 Saving the Entire Capture File using File > Save or the Save icon

This option is only available when you select Single File from the Capture Mode on System Settings. Click here to learn more about selecting Save options from System Settings.

1. If you are capturing data, click on the *Stop* icon  to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display*  or *Frame Display*  window.

3. Click the *Save* icon, or select *Save* from the *File* menu.

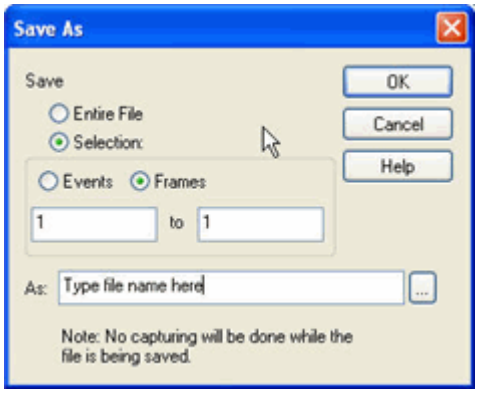


4. Type a filename in the *File name* box at the bottom of the screen.
5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.
6. When you are finished, click *OK*.

22.3 Saving the Entire Capture File with Save Selection

1. If you are capturing data, click on the *Stop* icon  to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display*  or *Frame Display*  window.
3. Right click in the data

4. Select *Save Selection* or *Save As* from the right click menu

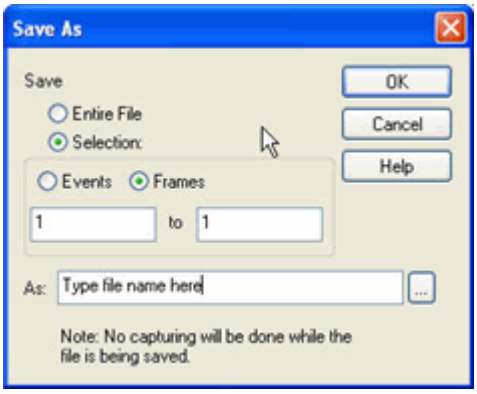


1. Click on the radio button labeled *Entire File*.
2. Choose to save *Events* or *Frames.* Choosing to save *Events* saves the entire contents of the capture file. Choosing to save *Frames* does not save all events in the capture file.
3. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
4. When you are finished, click *OK*.

22.4 Saving a Portion of a Capture File

1. If you are capturing data, click on the *Stop* icon  to pause data capture. You cannot save data to a file while it is being captured.
2. Open the *Event Display*  or *Frame Display* window  , depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the Frame Display toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Right click in the data

5. Select *Save Selection* or *Save As* from the right click menu



6. Click on the radio button labeled *Selection*. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.
7. Select either *Events* or *Frames* to indicate whether the numbers are event or frame numbers.
8. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
9. Click *OK* when you are finished.

22.5 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- Save To This File – Saves the changes you have made to the current capture file.
- Save As – Saves the changes to a new file.
- Cancel the Close Operation – Closes the file and returns you back to the display. No changes are saved.
- Discard Changes – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

22.6 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon  . This icon is present on the toolbars of the *Frame Display*  , the *Protocol Navigator*  , as well as the *Event Display*  . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon  to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

23 Loading and Importing Capture Files

23.1 Loading a Capture File

From the Control Window:

1. Go to the File menu.
2. Choose a file from the recently used file list.
3. If the file is not in the File menu list, select *Open Capture File* from the File menu or simply click on the *Open* icon  on the Toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click Open.

23.2 Importing Capture Files

1. From the Control Window  , go to the File menu and select *Open Capture File* or click on the *Open* icon on the Toolbar.
2. Change the Files of Type box to All Importable File Types or All Supported File Types. Select the file and click Open.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

At present, the analyzer supports the following file types:

- **Frontline Serialtest* Async and Serialtest ComProbe® for DOS** – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Greenleaf ViewComm* 3.0 for DOS** - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Frontline Ethertest* for DOS** – requires 3 files: filename.cap, filename.ca0 and filename.ca1.

- **Sniffer Type 1** – supports files with the .enc extension. Does not support Sniffer files with a .cap extension.
- **Snoop or Sun Snoop** – files with a .cap extension based on RFC 1761. For file format, see http://www.faqs.org/rfcs/rfc1761.html.
- **Shomiti Surveyor files in Snoop format** – files with a .cap extension. For file format, contact Technical Support.
- **CATC Merlin** - files with a .csv extension. Files must be exported with a specific format. See File Format for Merlin Files for information.
- **CATC Chief** - files with a .txt extension.

23.3 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

23.4 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon  . This icon is present on the toolbars of the *Frame Display*  , the *Protocol Navigator*  , as well as the *Event Display*  . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon  to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.

5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

23.5 File Format for Merlin Files

FTS imports Merlin's export files that have been exported with Merlin's default settings. These files should have an extension of ".csv".

It is possible with the Merlin software to hide or change a field's format. If you do this before exporting the Merlin file then FTS may have trouble importing the file.

If you are experiencing problems importing Merlin files, then check to make sure that no fields were hidden and that the default field formats were being used, when the file was exported from Merlin.

24 Printing

24.1 Printing from the Frame Display/HTML Export

The Frame Display Print dialog and the Frame Display HTML Export are very similar. This topic discusses both dialogs.

The **Frame Display Print** dialog is directly below. The **Frame Display HTML Export** is located midway in this discussion.

About Frame Display Print

The Frame Display Print feature provides the user with the option to print the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

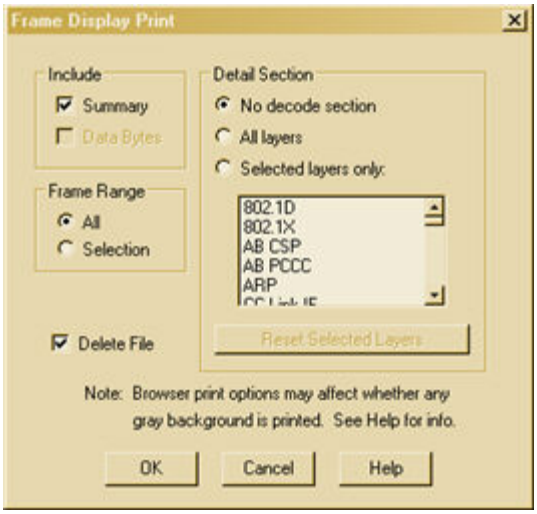
Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to *Selection* and allows the user to choose the *All* radio button. When only one frame is selected, the *All* radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select *Print* or *Print Preview* from the *File* menu on the Frame Display window to display the Frame Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

Choosing *All* prints all of the frames in the capture file or buffer. If more than 1000 frames in the Frame Range, All will be disabled. You can still select more than 1000 frames using the Selection option, but when printing more than 1000 frames, there is the possibility that Print will not work properly.

Choosing *Selection* prints only the frames you select in the Frame Display window.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

4. Click the OK button.

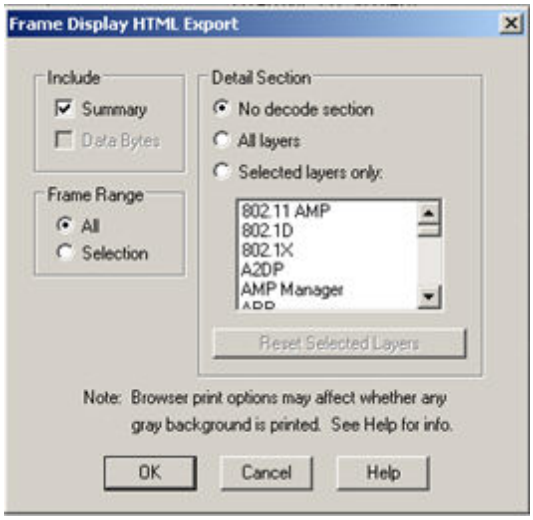
If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

24.2 Frame Display HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



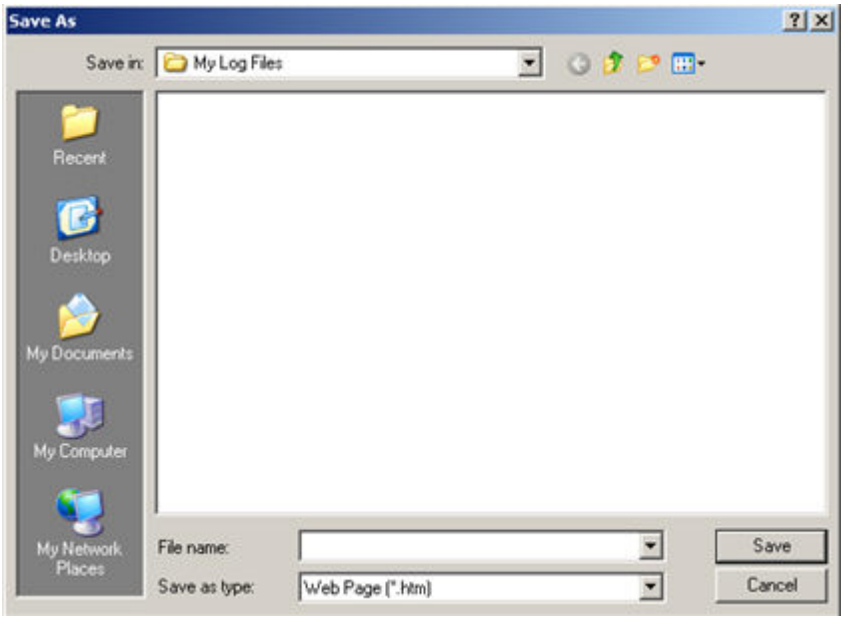
2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.
4. Select the range of frames to include *All* or *Selection* in the Frame Range section of the dialog.

   Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

Note: There is no need to choose a file type. The file is saved as a .htm.

7. Select Save

The file is saved as a .htm file in the file location you chose.

24.3 Printing from the Event Display

About Event Display Print

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

The Event Display Print feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the print feature.

Configure the Print File Range in the Event Display Print Dialog

Selecting more than one event in the Event Display window defaults the radio button in the Event Display Print dialog to Selection and allows the user to choose the All radio button. When only one event is selected (can't have None selected), the *All* radio button in the Event Display Print dialog is selected.

How to Print Event Display Data to a Browser

1. Select *Print* or *Print Preview* from the *File* menu on the Event Display window to display the Event Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Select the range of events to include from either *All* or *Selection* in the Event Range section of the Event Display Print dialog. Choosing *All* prints all of the events in the capture file or buffer. Choosing *Selection* prints only the selected events in the Event Display window.

   Note: In order to prevent a Print crash, you cannot select* All *if there are more than 100,000 events in the capture buffer.

Note: See Configure the Print File Range in the Event Display Print Dialog above for an explanation of these selections



3. Click the OK button.

If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

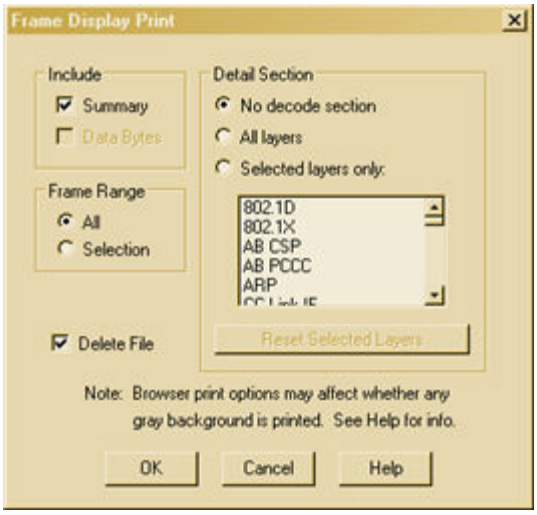
24.4 Print Preview

Print Preview gives a preview of how the data looks printed. You can scroll through the pages and zoom in on the data to get a closer look. The line of buttons across the top of the window controls the functions of the window.

To open the Print Preview window:

1. Choose Print Preview from the File menu in any window that supports printing.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



4. Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

   Choosing *All* prints all of the frames in the capture file or buffer. If there are more than 1000 frames in the capture file or buffer, **All** will not be available.

   Choosing *Selection* prints only the selected frames in the Frame Display window.

Note: See Configure the Print File Range in the Frame Display Print Dialog above for an explanation of these selections.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

5. Click the OK button.

You can print directly from the Print Preview window.

- Next Page shows you how the next page in your data looks
- Prev Page takes you back to the previous page.
- Two Page changes the display to show two pages of data. When in the Two Page display, the button reads One Page. Click on the One Page button to return to viewing one page.
- Zoom In and Zoom Out allow you to change the magnification of the pages. Click on Zoom In to increase the magnification, and on Zoom Out to decrease the magnification. When you have reached the limit in either direction, the buttons is grayed out.
- You can also zoom in and out by clicking on the page itself. When the cursor looks like a magnifying glass, you can click on the page to increase the magnification. When you have reached the top level of magnification, the cursor changes back to an arrow. Click on the page to return to normal magnification.
- Click on the Close button to return to the regular display.

25 Exporting

25.1 Export

You can dump the contents of the Summary pane on the Frame Display into a Comma Separated File (CSV).

To access this feature:

1. Right click on the Summary Pane
2. Select the Export menu item
3. Enter a file name
4. Select Save

Another option to access quick export is :

1. Click on the File menu
2. Choose Export
3. Enter a file name
4. Select Save

25.2 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the Filter Out box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

25.3 Exporting Event Display to a File

About Event Display Export

The Event Display Export feature provides the following options:

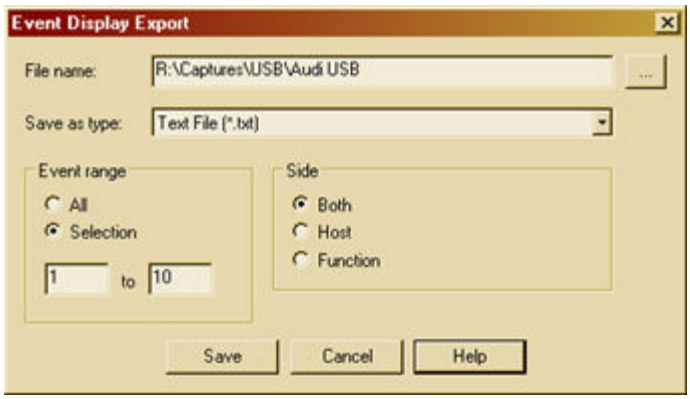
- Export either the entire capture buffer or the current selection
- Output file format as text, CSV, html, or bin.

The Event Display Export feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the export feature.

Accessing the Event Display Export Dialog

Selecting Export Events… from the File menu in the Event Display brings up the following dialog:



Configure the Export File Range in the Event Display Export Dialog

- Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.
- When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.
- Side is used to determine whether you want to export data from a DCE/DTE, Slave/Master, Host/Function device or both.

How to Export Event Display Data to a File

1. Select Export Events… from the File menu on the Event Display window to display the Event Display Export dialog.

2. Enter a file path and name, or click the browser button to display the Windows Save As dialog and navigate to the desired storage location.
3. Select a file type from the Save as type: drop-down List Menu on the Event Display Export dialog.
4. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

Binary File (*.bin)

5. Select the range of events to include in the file from either All or Selection in the Event Range section of the Event Display Export dialog.
   Note: See Configure the Export File Range in the Event Display Export Dialog above for an explanation of these selections.
6. Select a Side, either Host, Function, or Both
7. Click Save.

25.4 Exporting Baudot

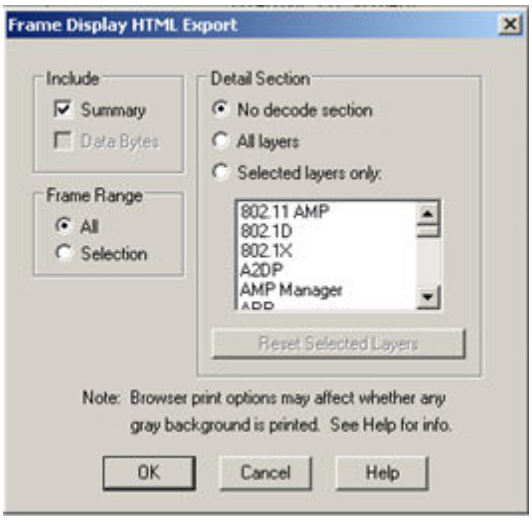
When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

25.5 HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the Data Bytes option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected

layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the Reset button to de-select all selected layers.

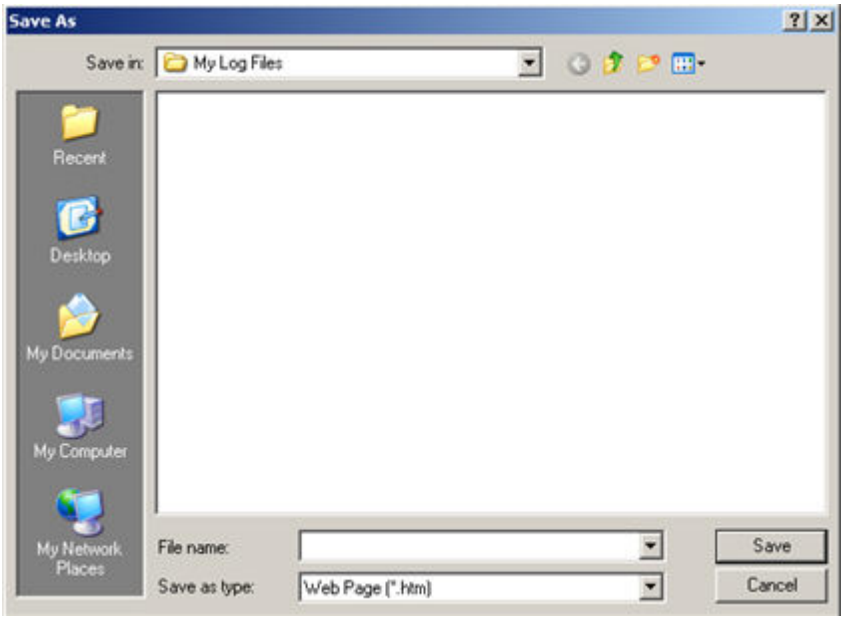
4. Select the range of frames to include All or Selection in the Frame Range section of the dialog.

   Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

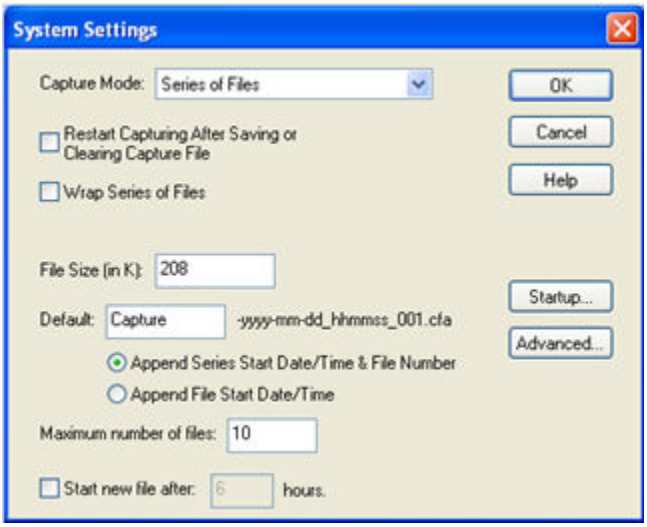
Note: There is not need to choose a file type. The file is saved as a .htm.

7. Select Save

26 System Settings and Program Options

26.1 System Settings

Open the System Settings window by choosing System Settings from the Options menu on the Control window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.



Capture Mode

- **Series of files**

  This option lets you capture to a series of files. The size of each file is no larger than the number given in File Size (in K),which has a maximum limit of approximately 176,000KB (1.7 GB) or 1/2 of the available hard disk space, whichever is **smaller**. The name of each file is the name you give it in the Name box followed by the date, time and a number. The date and time are when the series was opened. The number increments with each file. This guarantees unique file names are created.

  Set the maximum number of files in the series in the **Maximum number of files** box. The next file starts when the currently open file is full. If you want to start a new file on a periodic basis, check the box for **Start new file after** and put in the number of hours after which a new file is started. Note that if the currently open file becomes full before the time limit has been reached, a new file is opened immediately rather than lose data.

  Capturing stops if the maximum number of files has been used unless Wrap Files has been checked. If Wrap Files has been checked the analyzer erases the oldest file in the series and make a new file.

- **Single File**

This option allows the analyzer to capture data to a file without prompting you for a file name each time. The size of each file is not larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

Common Options

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size (in K)**

  Enter the maximum size of the capture file, which is 176,000 KB, or 1/2 of the available hard drive space, whichever is **smaller**. If you enter a number larger than the maximum allowable size, the analyzer will display the allowable size.

- **Default**
  Enter a name for the capture file in the Default text box. Each saved file will begin with this name.

- **Append Series Start/Date & File Number**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) and file number (001) when capturing a series of files.

- **Append File Start Date/Time**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) when capturing a single file.

- **Start up**

  Opens the Program Start up Options window. Start up options let you choose whether to start data capture immediately on opening the analyzer.

- Advanced

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

26.2 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the System Settings dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the Startup Options and Advanced System Options on the System Settings dialog and make changes to the settings at any time.

26.3 Bluetooth ComProbe Maintenance

The Bluetooth® ComProbe® Maintenance Utility is used to configure Bluetooth ComProbes and to upgrade the firmware. Bluetooth ComProbes should be upgraded to the newest firmware release to take advantage of new features and fixes.

Upgrading Your Bluetooth ComProbe

To start the Bluetooth ComProbe Maintenance Utility:

1. Open the FTS4BT desktop folder > Setup folder.
2. Double click the shortcut to the utility.

OR

1. From your Windows operating system click Start > Programs > FTS4BT [version#] > Setup > Bluetooth ComProbe Maintenance Utility.

The main dialog appears.

2. Connect the **ComProbe** to the PC
3. Click on the **Select Device** button.

To avoid mistakes, we recommended that only one ComProbe be connected at a time. Also, it is very important that you do not remove any connections to the ComProbe while the firmware update is in progress!

4. Select **Yes.**

Older ComProbes will display an error indicating the ComProbe is older and needs replacing. Note that when you do this, the [Device Information], [Check Configuration] and [Update Firmware] buttons should become available. [Update Firmware] will not be accessible if you are using an older ComProbe®.

5. Select the **Update Firmware** button.

The utility will display a dialog titled "Select the firmware file to download". There may be more than one firmware file with extension ".dfu" in the directory. The version number of the firmware will be in the name of the file.

6. Please **select the version you want** (typically you should choose the highest version number).
7. Then press the **Open** button.

When the update is complete, a dialog appears confirming the download.

8. Press the **OK** button.

26.4Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control  window.
2. Choose *System Settings* from the *Options* menu.
3. On the System Settings window, click the *Advanced* button.

- **Driver Receive Buffer Size in Kbytes**

  This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.

- **Driver Action Queue Size In Operating System Pages**

  This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.

- **Frame Completion Timeout in Seconds**

  This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

  If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

  Aborted frames (just like broken frames and regular frames) are decoded and displayed in the Frame Display. If you experience aborted frames and suspect that your framed data may have pauses in it that exceed the specified timeout time, then you may want to increase that value.

  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

  Note: This option is disabled when capturing data over Ethernet networks.

26.5 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose Directories from the Options menu on the Control  window to open the File Locations window.
2. Select the default location you wish to change.
3. Click Modify.
4. Browse to a new location.
5. Click OK.
6. Click OK when finished.

Note: If a user sets the **My Decoders** directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch FTS. For example, if an FTS product is installed at **C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z**, then "My Decoders" cannot be set to any of the following:

- C:\
- C:\FTS Stuff
- C:\FTS Stuff\My Products
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z

- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders
- or to any directory that already exists under C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders

Default Capture File Folder Checkbox

If the "Use Last Opened Folder for Capture Files" checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the **default** location for saving capture files is **Drive A > Folder A**. Now you select the "Use Last Opened Folder for Capture Files" checkbox. The next time, however, you open a capture file from a different location, **Folder B > Removable Flash Drive**. Now when you save the capture file, it will be saved to **Folder B > Removable Flash Drive**. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

There is one caveat to this scenario, however. Let's say you have selected "Use Last Opened Folder for Capture Files" and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. FTS will always try to save a file to the folder where the last file was opened from or saved to, if "Use Last Opened Folder for Capture Files" is checked. If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

26.6 Selecting Start Up Options

1. To open this window:
2. Choose *System Settings* from the *Options* menu on the Control  window.
3. On the System Settings window, click the *Start Up* button.
4. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

Don't start capturing immediately.

This is the default setting. The analyzer begins monitoring data but does not begin capturing data until the *Start Capture*  icon on the Control, Event Display or Frame Display windows is clicked.

Start capturing to a file immediately.

When the analyzer starts up, it immediately opens a capture file and begin data capture to it. This is the equivalent of clicking the *Start Capture*  icon. The file is given a name based on the settings for capturing to a file or series of files in the System Settings window.

Start capturing immediately to the following file:

Enter a filename in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

Use this capture filter:

The drop down box lists all named filters. Select one that you want to use immediately on start up.

26.7 Names

The Names dialog is used to change the names of objects and events that appear in various displays.

1. To open the Names dialog, choose *Names* from the *Options* menu on the Control window. Changes to the Names are used throughout the program.

To change a name, click on the name given in the current column, and then click again to modify the name (a slow double-click). To restore the default values, click the Defaults button. The names used in the system fall into one of three general categories.

Because of variations associated with different types of communications, the Names dialog may display all or only a subset of the following categories:

- **Sides**

  The Sides section allows you to give each side on a network more descriptive names. This is useful on network with more than one side.

- **Errors**

  This section allows you to change the error names. The errors listed are appropriate for the type of circuit/network you are monitoring.

- **Signals**

  Signals refers to the six control signals used in RS-232 data communications, and may not apply to the type of communications you are monitoring.

  FTS4USB has four Control Signals: Pin 1, Pin 2, Pin 3, and Pin 4.

  Default Labels and their Meaning

Label	Control Signal
RTS	Request to Send

CTS	Clear to Send
DSR	Data Set Ready
DTR	Data Terminal Ready
CD	Carrier Detect
RI	Ring Indicator

If you are used to different abbreviations for the same signals, you can change them in this section. For example, if you normally refer to Carrier Detect as DCD, highlight CD and type in DCD.

26.8 Timestamping

26.8.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

1. Choose *System Settings* from the *Options* menu on the Control window.
2. Click the *Set Timestamp Format* button.

OR

1. Click the Timestamping Options icon from either the Event Display or Statistics window.

OR

1. Click the Timestamping Options icon from the Event Display window.

26.8.2 Enabling/Disabling Timestamping

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.

2. Check the *Store Timestamps* box to enable timestamping. Remove the check to disable timestamping. If you disable timestamping, you are not able to do delta or rate calculations.

26.8.3 Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Statistics  window.
2. Go to the *Display Options* section at the bottom of the window and find the *Display Relative Timestamps* checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Note: The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- *Display Raw Timestamp Value* shows the timestamp as the **total time in hundred nanoseconds** from a specific point in time.
- *Display Relative Timestamps* shows the timestamp as the **amount of time that has passed since the first byte was captured**. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.
- *Selecting both values* displays the **total time in nanoseconds from the start of the capture** as opposed to a specific point in time.
- *Selecting neither value* displays the **actual chronological time**.

When you select Relative Timestamp, you can set the number of digits to display using the up or down arrows on the numeric list.

26.8.4 Changing the Timestamping Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.

2. Go to the *Capture Options* section of the window.
3. Change the resolution listed in the *Storage Resolution* box. Note that if you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

26.8.5 Displaying Fractions of a Second

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.
2. Go to the *Display Options* section at the bottom of the window, and find the *Number of Digits to Display* box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

The options in this section affect only how the timestamps are displayed on the screen, not the resolution used to capture the data.

26.8.6 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

26.8.7 Performance Issues For High Resolution Timestamps

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are

required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

27 Technical Information

27.1 Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://www.fte.com/support/default.asp

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

27.2 Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Buffer overflow errors are an indicator that the analyzer is unable to keep up with the data. The information below describes what happens to the data as it arrives, what the error means, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

The analyzer's driver takes data from the driver and counts each byte as they are put into the driver's buffer. The analyzer's driver tells the user interface that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

Driver Buffer Overflows occur when the user interface does not retrieve frames from the driver quickly enough. Buffer overflows are indicated in the Event Display window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost.

There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by the analyzer. (Ethernet Only)
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the Event Display window or other processor intensive activities while the analyzer is capturing data.

- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the file. Try turning off timestamping from the Timestamping Options window.
- For Driver Buffer Overflows, change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value Driver Receive Buffer Size in Operating System Pages. Take the number listed there and double it.
- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. The analyzer can capture data with no windows other than the Control window open.
- If you are still experiencing buffer overflows after trying all of the above options, then you need to use a faster PC.

27.3 Asynchronous Serial Performance Notes

As a software-based product, the speed of your computer's processor affects FTS's performance. Overrun errors and buffer overflows are indicators that FTS is unable to keep up with the data. The information below describes what happens to the data as it comes in the port, what the two types of errors mean, and how various aspects of FTS affect performance. Also included are suggestions on how to improve performance.

Data captured by the serial port first goes into the buffer of the UART chip of the serial port. The UART generates an interrupt, which tells the FTS driver to check the port. The driver takes the data from the UART and counts each byte as they are put into the driver's own buffer. The driver tells FTS that data is ready to be processed. FTS takes the data from the driver's buffer and puts the data into the capture buffer.

Overrun errors occur when the data in the buffer of the UART is not retrieved before new data comes in. In this case, FTS knows that it has lost information, but it does not know how much. FTS indicates overrun errors in the Event Display screen by marking a byte near the overrun in red. You can search for overrun errors using the Find feature.

Driver buffer overflow errors occur when the data in the buffer of the driver is not retrieved before new data comes in. Since the driver counts the bytes as it retrieves them from the UART, it not only knows that it has lost data, it also knows how much. Buffer overflows are indicated in the Event Display screen by a plus sign within a circle. Clicking on the buffer overflow symbol shows how many events have been lost. The Statistics window is a good place to check for buffer overflow errors.

Both overrun errors and buffer overflows indicate that data is coming in too quickly for FTS to process. There are several things that you can do to try and solve this problem.

- In the Hardware Settings window, select *Use Windows Device Manager Settings*. This means that Windows does not generate an interrupt every time a byte comes in, but rather waits until several bytes have accumulated in the UART buffer before telling FTS to retrieve them. This increases performance at the cost of timestamp accuracy, since all the bytes in a group have the same timestamp regardless of when they actually arrived at the UART. Some control signal changes may also be lost.
- FTS's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause FTS to lose data while the window is being updated. Some windows require more processing time than others, because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. Try closing the Breakout Box and Statistics windows. FTS can capture data with no windows other than the Control window open.
- Increase the value of the window refresh rate for any windows you have open while capturing data. This decreases the frequency of window updates, leaving more time for capturing data. Changing the refresh rate can be done from the Options screen in each window.
- If you suspect or know that your circuit has control signals that are changing very rapidly, go to the Hardware Settings window and choose to Disable Control Signal Interrupts. This prevents FTS from capturing control signal changes on an interrupt basis, giving more time for capturing byte data. (You can use the counters in the Breakout Box to help determine if a control signal is changing quickly.) FTS still notes the state of the control signals whenever a byte is captured. You must restart FTS for this change to take effect.
- Close all other programs that are working while FTS is running. Refrain from doing searches in the Event Display window or other processor intensive activities while FTS is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the buffer or file. Try turning off timestamping from the Timestamping Options window.
- Change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value labeled Driver Receive Buffer Size in Operating System Pages. Take the value listed there and double it.

  NOTE: This procedure might help buffer overflow errors, but does not help overrun errors.

- Slow down the speed of the communications circuit, if possible.

If you are still experiencing overruns and/or buffer overflows after trying all of the above options, then you may need to use a faster PC.

27.4 Synchronous Serial Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Overrun errors and buffer overflows are indicators that the analyzer is unable to keep up with the data. Underrun errors occur when the analyzer is unable to transmit data quickly enough when transmitting synchronous data. The information below describes what happens to the data as it comes in the ComProbe®, what the three types of errors mean, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

Data captured by the ComProbe first goes into the buffer of the Universal Synchronous/Asynchronous Receiver Transmitter (USART) chip of the ComProbe. The USART generates an interrupt, which tells the analyzer driver to check the ComProbe. The driver takes the data from the USART and counts each byte as they are put into the driver's own buffer. The driver tells the analyzer that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

USART Overrun errors occur when the data in the buffer of the USART is not retrieved before new data comes in. In this case, the analyzer knows that it has lost information but it does not know how much. The analyzer indicates overrun errors in the Event Display screen by marking a byte near the overrun in red. You can search for overrun errors using the Find feature.

Driver buffer overflow errors occur when the data in the buffer of the driver is not retrieved before new data comes in. Since the driver counts the bytes as it retrieves them from the USART, it not only knows that it has lost data, it also knows how much. Buffer overflows are indicated in the Event Display screen by a plus sign within a circle. Clicking on the buffer overflow symbol shows how many events have been lost. The Statistics window is a good place to check for buffer overflow errors.

Underrun errors occur only in synchronous source mode. If the analyzer cannot keep the transmit buffer supplied with enough data, it sends non-data characters instead, and may mark the next transmitted byte as an underrun error.

All three errors indicate that data is coming in or going out too quickly for the analyzer to process. There are several things that you can do to solve this problem.

- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others, because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. Try closing the Breakout Box and Statistics windows. The analyzer can capture data with no windows other than the Control window open.
- Increase the value of the window refresh rate for any windows you have open while capturing data. This decreases the frequency of window updates, leaving more time for capturing data. Changing the refresh rate can be done from the Options screen in each window.

- If you suspect or know that your circuit has control signals that are changing very rapidly, go to the Hardware Settings window and choose to Disable Signal Interrupts. This prevents the analyzer from capturing control signal changes on an interrupt basis, giving more time for capturing byte data. (You can use the counters in the Breakout Box to help determine if a control signal is changing quickly.) The analyzer still notes the state of the control signals whenever a byte is captured. You must restart the analyzer for this change to take effect.
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the Event Display window or other processor intensive activities while the analyzer is capturing data.
- Change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value labeled Driver Receive Buffer Size in Operating System Pages. Take the value listed there and double it. **NOTE:** This procedure might help buffer overflow errors, but does not help overrun errors.
- Slow down the speed of the communications circuit, if possible.

If you are still experiencing overruns and/or buffer overflows after trying all of the above options, then you may need to use a faster PC.

27.5 Ethernet Performance Notes

As a software-based product, the speed of your computer's processor affects FTS's performance. Receive overrun, frames missed and buffer overflow errors are indicators that FTS is unable to keep up with the data. The information below describes what happens to the data as it arrives at the network card, what the types of errors mean, and how various aspects of FTS affect performance. Also included are suggestions on how to improve performance.

Data captured by the network card first goes into the card's buffer. The card generates an interrupt, which tells the NDIS driver to check the port. The FTS driver takes the data from the NDIS driver and counts each byte as they are put into the FTS driver's buffer. The FTS driver tells the FTS user interface that data is ready to be processed. FTS takes the data from the driver's buffer and puts the data into the capture file.

Receive overruns occur when the frame buffer on the network card is not emptied by the NDIS driver. Frames missed and no buffer errors occur when the FTS driver does not clear out the NDIS driver buffer. In both of these situations, FTS knows that it has lost data, but does not know how much.

Driver Buffer Overflows occur when the FTS user interface does not retrieve frames from the FTS driver quickly enough. The Frames Lost counter on the Statistics window displays the number of frames lost due to driver buffer overflows. Since the driver counts the frames as it retrieves them from the NDIS driver, it not only knows that it has lost data, it also knows how much. Buffer overflows are indicated in the Event Display window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost. The Statistics window is a good place to check for buffer overflow errors.

All 3 types of errors indicate that data is coming in too quickly for FTS to process. There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by FTS.
- Close all other programs that are doing work while FTS is running. Refrain from doing searches in the Event Display window or other processor intensive activities while FTS is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the buffer or file. Try turning off timestamping from the Timestamping Options window.
- For Driver Buffer Overflows, change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value Driver Receive Buffer Size in Operating System Pages. Take the number listed there and double it.
- For Frames Missed and No Buffer errors, change the number of NDIS buffers. To do this, choose Hardware Settings from the Options menu on the Control window, and double the value listed in Number of NDIS buffers to use.
- FTS's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause FTS to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. Try closing the Statistics windows. FTS can capture data with no windows other than the Control window open.
- If you are still experiencing receive overruns, frames missed errors and/or buffer overflows after trying all of the above options, then you have to use a faster PC.

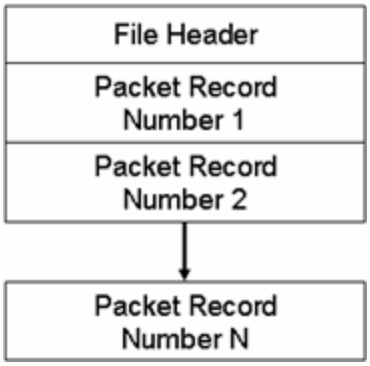
27.6BT Snoop File Format

Overview

The BT Snoop file format is suitable for storing *Bluetooth*® HCI traffic. It closely resembles the snoop format, as documented in RFC 1761.

File Format

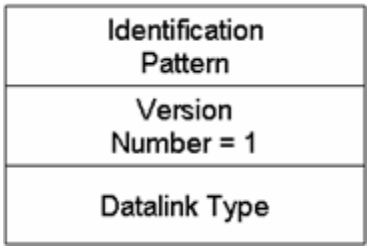
The snoop packet capture file is an array of octets structured as follows:



The File Header is a fixed-length field containing general information about the packet file and the format of the packet records it contains. One or more variable-length Packet Record fields follow the File Header field. Each Packet Record field holds the data of one captured packet.

File Header

The structure of the File Header is as follows:



Identification Pattern:

A 64-bit (8 octet) pattern used to identify the file as a snoop packet capture file. The Identification Pattern consists of the 8 hexadecimal octets:

62 74 73 6E 6F 6F 70 00

This is the ASCII string "btsnoop" followed by one null octets.

Version Number:

A 32-bit (4 octet) unsigned integer value representing the version of the packet capture file being used. This document describes version number 1.

Datalink Type:

A 32-bit (4 octet) field identifying the type of datalink header used in the packet records that follow. The datalink type codes are listed in the table below. Values 0 - 1000 are reserved, to maximize compatibility with the RFC1761 snoop version 2 format.

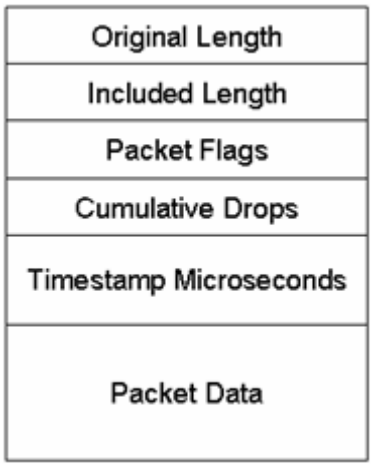
Datalink Type	Code
Reserved	0 - 1000
Un-encapsulated HCI (H1)	1001
HCI UART (H4)	1002
HCI BCSP	1003
HCI Serial (H5)	1004
Unassigned	1005 – 4294967295

Packet Record Format

Each packet record holds a partial or complete copy of one packet as well as some descriptive information about that packet. The packet may be truncated in order to limit the amount of data to be stored in the packet file.

Each packet record holds 24 octets of descriptive information about the packet, followed by the packet data, which is variable-length, and an optional pad field. The descriptive information is structured as six 32-bit (4-octet) integer values.

The structure of the packet record is as follows:



Original Length

A 32-bit unsigned integer representing the length in octets of the captured packet as received via a network.

Included Length

A 32-bit unsigned integer representing the length of the Packet Data field. This is the number of octets of the captured packet that are included in this packet record. If the received packet was truncated, the Included Length field is less than the Original Length field.

Packet Flags

Flags specific to this packet. Currently the following flags are defined:

Bit no	Definition
0	Direction flag. 0 = Sent; 1 = Received
1	Command flag. 0 = Data; 1 = Command/Event
2 – 31	Reserved.

Bit 0 is the least significant bit of the 32-bit word.

Direction is relative to host / DTE. i.e. for *Bluetooth* controllers, Send is Host->Controller, Receive is Controller->Host.

Note: Some Datalink Types already encode some or all of this information within the Packet Data. With these Datalink Types, these flags should be treated as informational only, and the value in the Packet Data should take precedence.

Cumulative Drops

A 32-bit unsigned integer representing the number of packets that were lost by the system that created the packet file between the first packet record in the file and this one. Packets may be lost because of insufficient resources in the capturing system, or for other reasons.

Note: some implementations lack the ability to count dropped packets. Those implementations may set the cumulative drops value to zero.

Timestamp Microseconds

A 64-bit signed integer representing the time of packet arrival, in microseconds since midnight, January 1st, 0 AD nominal Gregorian.

In order to avoid leap-day ambiguity in calculations, note that an equivalent epoch may be used of midnight, January 1st 2000 AD, which is represented in this field as 0x00E03AB44A676000.

Packet Data

Variable-length field holding the packet that was captured, beginning with its datalink header. The Datalink Type field of the file header can be used to determine how to decode the datalink header. The length of the Packet Data field is given in the Included Length field.

Note that the length of this field in not necessarily rounded to any particular multi-octet boundary, as might otherwise be suggested by the diagram.

Data Format

All integer values are stored in "big-endian" order, with the high-order bits first.

27.7 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

27.8 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

27.9 Event Numbering

This section talks about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

When the analyzer captures an *event*, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are *wrapped* out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file use the same event numbers that your file does.

27.10 File Format for Merlin Files

FTS imports Merlin's export files that have been exported with Merlin's default settings. These files should have an extension of ".csv".

It is possible with the Merlin software to hide or change a field's format. If you do this before exporting the Merlin file then FTS may have trouble importing the file.

If you are experiencing problems importing Merlin files, then check to make sure that no fields were hidden and that the default field formats were being used, when the file was exported from Merlin.

27.11 Flag and Sync Character Subtleties

The chip used by the ComProbe® hides some details relating to HDLC/SDLC flags (hex 7e) and the sync character in Bisync and Monosync.

In HDLC and SDLC, the analyzer does not know how many flag characters were actually present between frames. The analyzer inserts a 7e at the start and end of each frame to indicate that at least one flag was present on the link. What FTS shows is:

<7e><start-of-frame marker><data><crc><end-of-frame marker><7e><7e><start-of-frame marker><data><etc.>

However, there may have been many flags between frames or just one, but the analyzer has no way to know this.

In Bisync and Monosync, the chip hides the characters used as sync characters. The analyzer displays at least two syncs in Bisync and one in Monosync to show that sync characters were present, but the analyzer does not know how many syncs actually occurred. One result of this is that the timestamps on the sync characters may not be correct since the analyzer only knows that the sync characters occurred when data comes in.

27.12 Known Issues with the Source BD_ADDR Field

The data contained in the Source BD_ADDR field has the potential to be inaccurate.

A number of factors associated with wireless communication such as complex usage scenarios, or dropped data packets due to poor RF reception contribute to incorrect information periodically appearing in this field. Due to the nature of wireless communication, it is not always possible for the analyzer, or any device, to determine the BD_ADDR of the communicating devices on the network.

Users should keep in mind that the data contained in the Source BD_ADDR field should be used as a guide and not an absolute.

27.13 Ring Indicator

The following information applies when operating the analyzer in *Spy* mode or *Source DTE, No FTS Cables* mode. When using the cables supplied with the analyzer to capture or source data, *Ring Indicator* (RI) is routed to a different pin which generates interrupts normally.

There is a special case involving Ring Indicator and computers with 8250 *UART*s or UARTs from that family where the state of RI may not be captured accurately. Normally when a control signal changes state from high to low or low to high, an interrupt is generated by the UART, and the analyzer goes to see what has changed and record it. Ring Indicator works a little differently. An interrupt is generated when RI changes from high to low, but not when RI changes from low to high. If Ring Indicator changes from low to high, the analyzer does not know that RI has changed state until another *event* occurs that generates an interrupt. This is simply the way the UART works, and is not a deficiency in the analyzer software.

To minimize the chance of missing a Ring Indicator change, the analyzer polls the UART every millisecond to see if RI has changed. It is still possible for the analyzer to miss a Ring Indicator change if RI and only RI changes state more than once per millisecond.

UARTs in the 8250 family include 8250s, 16450s, 16550s and 16550 variants. If you have any questions about the behavior of your UART and Ring Indicator, please contact technical support.

27.14 Padding of Short Frames

Ethernet requires that frames be a minimum of 60 bytes in length, not including the CRC. If the frame is less than 60 bytes, the NIC pads it before putting it on the wire. Pad characters are usually nulls (hex 00).

Frames transmitted by the PC running the analyzer are looped back by the NDIS driver so the transmitting PC can see the frame. The loopback occurs before the NIC has added any necessary padding to the end of the frame. The analyzer compensates for this by using the sequence "Pad", repeated as many times as necessary, as a placeholder. The analyzer uses only as many characters as needed to bring the frame up to the required 60 bytes, so you may see partial "Pad"s or multiple "Pad"s. For example, you may see "PadPadPad", "PadPa" "Pa", etc.

27.15 RS-232 Pin-outs

25-pin connector

Pin	Name	Abbreviation
1	Frame Ground	FG
2	Transmit Data	TxD
3	Receive Data	RxD
4	Request To Send	RTS
5	Clear to Send	CTS
6	Data Set Ready	DSR
7	Signal Ground	GND
8	Carrier Detect	CD or DCD
20	Data Terminal Read	DTR
22	Ring Indicator	RI

9-pin connector

Pin	Name	Abbreviation
1	Carrier Detect	CD or DCD
2	Receive Data	RxD
3	Transmit Data	TxD
4	Data Terminal Ready	DTR
5	Signal Ground	GND
6	Data Set Ready	DSR
7	Request To Send	RTS
8	Clear To Send	CTS
9	Ring Indicator	RI

27.16 CRC!

When NDIS receives a frame, it checks that the CRC is good and then discards it before passing the frame up to the next higher layer. The analyzer adds "CRC!" to the end of Ethernet frames to compensate.

NDIS does not pass up frames with bad CRCs, so there is no way for the analyzer to capture them. Some (but not all) NDIS drivers record the number of frames received with bad CRCs. The number of CRC errors is shown in the Errors table on the Statistics window.

To manually determine the CRC for a frame, use the CRC function on the Event Display.

27.17 BPF Copyright Notice

This copyright applies to code used in the filter feature. Filtering functionality in FTS is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump.

Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997

The Regents of the University of California. All rights reserved.

This code is derived from the Stanford/CMU enet packet filter, (net/enet.c) distributed as part of 4.3BSD, and code contributed to Berkeley by Steven McCanne and Van Jacobson both of Lawrence Berkeley Laboratory.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
- Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

27.18 Useful Character Tables

27.18.1 ASCII Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

27.18.2 Baudot Codes

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

27.18.3 EBCDIC Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

27.18.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File

		Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

27.19 The Serial Driver

27.19.1 The FTS Serial Driver

FTS uses custom versions of the standard Windows serial drivers in order to capture data. These drivers are usually installed during the routine product installation. However, if you need to install the serial driver after FTS has already been installed, please refer to the

instructions available in the Setup folder installed under Start | Programs | [Product Name and version #] | Setup | How to Install the FTS Serial Driver.

27.20 Frame Decoder

Frame Decoder is for the development of add-on components to extend the functionality of your FTS protocol analyzer. Those add-on components are generally used to decode existing or custom protocols. The core of each such "decoder" is a program that defines how the protocol data are to be broken up into fields and displayed in the Frame Display window of the analyzer software. The DecoderScript Manual provides instruction on how to create custom decoders and use them just like any of the decoders supplied with the protocol analyzer. You can also apply this knowledge to modify decoders supplied with the protocol analyzer.

For more information about Frame Decoder, consult the DecoderScript Manual located in the desktop folder under Optional Components, or simply select *Start | Programs | Frontline [Product Name and Version Number] | Optional Components | DecoderScript Manual*.

28 Index

A

A2DP Decoder Parameters · 18
About Display Filters · 267
About Statistics · 137
Absolute Time · 321
Absolute Timestamp Search · 261
Active Devices · 150
Active Devices Grid · 151
Active Devices Grid Buttons · 151
Add a New or Save an Existing Template · 47
Add/Edit an Alias for a Node in Network View · 218
Adding a New Predefined Stack · 91
Adding Comments To A Capture File · 295, 298
Advanced Display Filtering Techniques · 271
Apply Capture Filters · 59, 267, 268, 274, 275, 276, 277, 278, 279, 285, 286
Apply Display Filters · 267, 268, 269, 270, 271, 272, 273, 274
ASCII · 102, 258
  character set · 338
  removing the numbers on the Event Display · 102
  searching for ASCII strings · 258
  transmitting in · 173
  viewing data in · 102
ASCII Codes · 338
ASCII Pane · 117
Asynchronous Serial Performance Notes · 326
Audio Extraction · 242
Automatically Request Missing Decoding Information · 94
Auto-Sizing Column Widths · 114
Auto-traversal · 91
AVDTP · 20, 21, 22, 23, 24
AVDTP Override Decode Information · 24
AVDTP Parameter · 21, 22
  Add · 21
  Delete · 22
AVDTP Parameter Template · 20, 22, 23
  Add · 22
  Apply · 20
  Delete · 23
Average Throughput Indicators
  Average_Throughput_Indicators · 201

B

Backward Compatibility · 171
Bar Charts · 138
Baudot · 102, 173, 311
Baudot Codes · 339
BD_ADDR · 335
Berkeley Packet Filtering · 277
Binary · 257, 259
Binary Pane · 118
Bookmarks · 265, 266, 288
Boolean · 269, 273
BPF · 277
Breakout Box · 130, 131
  Breakout Box Options · 131
Buffer · 292
  Buffer Tabs · 137
Busy Tokens · 158
Byte · 118, 334
  Byte Count · 160
  Bytes Per Second Table · 140

C

Calculating Data Rates and Delta Times · 101
Capture Buffer · 292
Capture File · 174, 292, 294, 295, 298
  changing default location of · 317
  loading · 297
  removing framing markers · 93
  saving · 292
  transmitting · 174
Capture Filters · 267, 274, 275, 276, 278, 279, 285, 286
Capturing · 54
  ControlNet Data · 54
CFA file · 294, 295, 298
Changing Default File Locations · 317
Character · 257, 258
  Character Pane · 117
Character Set · 102, 338, 339
Character Strings in Searching · 258
Characters Per Second Table · 138
Coexistence View Introduction · 181
  Coexistence button bar · 186
Color of Data Bytes · 118
Colors · 119

Column Width · 114
Comma Separated File · 309
Compound Display Filters · 269
Compound Ethernet Capture Filters · 278
Confirm CFA Changes · 294
Context For Decoding · 94
Control Characters · 173, 259
Control Signals · 131, 133, 134, 136, 319
Control Window · 5, 10
  Configuration Information · 5
  Control Window Toolbar · 3
ControlNet · 54, 59
  ControlNet I/O Settings · 55
ControlNet 1784-U2CN Hardware Settings · 62
ControlNet 1784-U2CN I/O Settings · 63
Conversation Capture Filters · 276
Conversation Filters · 270
Copying Statistics · 138
CSV Files · 309
Custom Protocol Stack · 91
Custom Stack · 91
Customizing Fields in the Summary Pane · 114

D

Dashboard
  Dashboard - Define Authorized IP Addresses · 238
  Dashboard - Show IP Addresses Seen · 239
  Network View Dashboard · 231
Data · 101, 291, 292
Data Byte Color Denotation · 118
Data Extraction · 243
Data Rates · 101
Decode Pane · 116
Decodes · 94, 107, 116, 253
Default File Locations · 317
Delete a Template · 47
Deleting Display Filters · 271
Delta Times · 101
Device Token Rotations · 158
Devices Grid · 150
Difference Between Ethernet Capture Filters · 267
Direction · 270
Directories · 317
Disabling · 320
Discontinuities · 203
Display Conversation Information in Network View · 217
Display Entire Buffer · 134
Display Filters · 267, 272, 273, 274
Display Options · 154, 322
Dots · 115
Driver · 341
Duplicate View · 99, 112

E

Easy Protocol Filtering · 119, 286
EBCDIC · 102
  EBCDIC Codes · 339
Enabling/Disabling Timestamping · 320
Errors · 119, 121, 125, 288, 289, 319
Ethernet Capture Filter · 274, 275, 277, 278, 279, 285, 286
Event Display · 112, 304, 309
  Event Display Export · 309
  Event Display Print · 304
  Event Numbering · 334
  Event Pane · 118
Exclude · 268
Exclude Radio Buttons · 268
Expand All/Collapse All · 116
Expand Decode Pane · 113
Export
  Export Baudot · 311
  Export Events… · 309
  Export Filter Out · 309
  Export WAV File · 242

F

Field Width · 114
File · 174, 278, 286, 291, 292, 297
File Format Required for Merlin Capture Files · 299, 334
File Locations · 317
Filtering · 119, 218, 276, 286, 289
Filters · 119, 121, 124, 125, 218, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 285, 286, 288, 289
Find · 253, 257, 258, 259, 260, 261, 262, 263
Flow Control · 177
Font Size · 105
Fractions Of A Second · 322
Frame Display · 107, 111, 112, 113, 114, 115, 116, 117, 118, 119
  Frame Display Status Bar · 111
  Frame Display Window · 107
  Frame Symbols · 115
Frame Display - Right Click Filtering · 116, 121
Frames Per Second Table · 140
Freeze · 101
FTS Serial Driver · 341
FTS4USB Hardware Settings · 11
FTS4USB I/O Settings · 14

G

Graph Refresh Rate · 139
Graphs · 138, 139
Green Dots in Summary Pane · 115

H

Hardware Settings · 11
Hex · 259
Hexadecimal · 117
Hiding · 124
Hiding Display Filters · 271, 272
Hiding Layers · 124
High Resolution Timestamping · 321, 322

I

I/O Settings · 55
Include · 268
Include/Exclude · 268
Information Screen · 90
IP Address
  Filter · 276

L

L2CAP · 26, 27, 28, 29
  L2CAP Parameter · 27, 28
    Add · 27
    Delete · 28
  L2CAP Parameter Template · 26, 28, 29
    Add · 28
    Delete · 29
Layer · 124
Layer Colors · 119
Live Update · 101
Load Filter File · 286
Low Energy Timeline
  Average Throughput Indicators · 211
  Button Bar/Legend · 206
  Discontinuities · 214
  Legend · 214
  Navigating and Selecting Data · 205
  Once Second Throughput Indicators · 211
  Throughput Display · 211
  Throughput Graph · 213
  Timeline Menu Bar · 207
  Timeline Packet Depiction · 204
  Visual Elements · 208
  Zooming · 210

M

MAC Address Filter · 276
Menus · 4
Merlin Files · 299, 334
Minimizing · 10
Missing Decode Information · 24, 36
Mixed Channel/Sides · 103
Mixed Sides Mode · 103
Modem Lead Names · 319
Modem Leads · 133
Modify Capture Filters · 275, 278, 279
Modify Display Filters · 273, 274
Multiple Event Displays · 99
Multiple Frame Displays · 112

N

Named Filters · 278, 289
Names · 319
NetDecoder 1784-U2DN IO Settings Start Triggers · 74
Network Bytes Sent · 159
Network Bytes Sent Totals · 160
Network View Dashboard · 231
  Define Authorized IP Addresses · 238
  Show IP Addresses Seen · 239
Network View Introduction · 215
Network View Technical Notes · 226
New Snapshot · 134
Node Capture Filters · 276
Node Database · 223
Node Filters · 218, 270
Nonprintables · 309
Notes · 295, 298
Numbers · 334

O

Octets Per Second Table · 143
Offset · 277
Offset Ethernet Capture Filters · 277
Open · 99, 286
  Open Capture File · 297
Options · 131, 136, 154, 180, 318, 320
Override Decode Information · 24, 36
Overriding Frame Information · 94

P

Packet Error Rate · 147
Packet Timeline · 195, 203

Packet Timeline Menu Bar · 196
Packet_Timeline_Introduction · 191
Packet_Timeline_Visual_Elements · 198
Panes · 113
Parameter Template · 38, 40, 41
Parameters · 38
Pattern · 173, 257, 277
Pattern Ethernet Capture Filters · 277
Percentages · 139
Performance Issues For High Resolution Timestamps · 322
Performance Notes · 325, 326, 329
Physical Errors · 119
Pie Charts · 138
Predefined · 276
Predefined Ethernet Capture Filters · 276
Printing · 139, 304
Printing from the Frame Display · 301
Progress Bars · 334
Protocol
  Protocol Layer Colors · 119
Protocol List · 10
Protocol Navigator · 121
Protocol Stack · 91, 92

Q

Quick Export · 309
Quick Filtering · 121, 288

R

Radix · 117
Red Frame Numbers · 119
Relative Time · 260, 321
Relative Timestamp Search · 262
Remove
  Bookmarks · 265
  Columns · 114
  Filters · 271, 272, 275
  Framing Markers · 93
Renaming · 274
Reset Panes · 113
Resetable Tab · 137
Resolution · 321
Resolving DNS Names in Network View · 224
Revealing Display Filters · 272
Revealing Layers · 124
Revealing Protocol Layers · 124
RFCOMM · 32, 33, 34, 35, 36
RFCOMM Missing Decode Information · 36
RFCOMM Override Decode Information · 36
RFCOMM Parameter · 33
  Delete · 33
RFCOMM Parameter Template · 32, 34, 35
  Add · 34
  Apply · 32
  Delete · 35
ROC · 38, 39, 40, 41
ROC Parameter · 39, 40
  Delete · 39
  Edit · 40
ROC Parameter Template · 38, 40, 41
  Add · 40
  Delete · 41

S

Save · 268, 285, 291, 292
Save As · 291
Saving · 285, 291, 292
  Display Filter · 268
Saving the Capture File using File > Save or the Save icon · 291
Search · 253, 257, 258, 259, 260, 261, 262, 263, 266
  binary value · 257
  bookmarks · 266
  character string · 257
  control characters · 259
  entering character strings · 258
  hex or binary characters · 259
  hex pattern · 257
  pattern · 257
  strings in decodes · 253
  timestamp · 260
  wildcards · 257
Send · 173, 180
  file · 174
  string · 173
Serial Driver · 341
Set The Count For Top N Filters · 219
Sides · 319
Signal Display · 133, 134
Signal Display Options · 136
Signal Display Toolbar · 134
Sorting Frames · 112
Source BD_ADDR · 335
Source BD_ADDR Field · 335
Spy · 49
Spy Mode Settings · 49
Start Up Options · 318
Starting DH+ Statistics · 149
Statistics · 137
Statistics Graphs · 138
Strings · 173
Summary Layer Protocol · 119, 286
Summary Pane · 114, 115

Synchronization · 112

T

Template · 22, 23, 33
Templates · 20, 28, 29, 32, 34, 35, 41, 44, 45
The Network View Toolbar · 224
Throughput Displays
  Throughput_Displays · 201
Throughput Graph · 202
Timestamp · 261, 262, 263, 321, 322
Timestamping · 262, 320, 322
Timestamping Options · 320
Timestamping Resolution · 321
Timestamps · 320, 322
Token · 158
Top Conversations Dialog · 165
Top Listeners · 169
Top Talkers · 152, 164
Transmit · 173, 174, 177, 180
Transmit Options · 180
Transmit Toolbar · 175
Transmit Window · 173
Transmitting · 174
Transmitting Frames · 174
Troubleshooting · 335

U

Unframe · 93
Unframe Function · 93
Unframing · 93
USB · 42, 44, 45, 96
USB ComProbe · 11, 14
USB HCI Internal Software Tap Data Source Dialog · 96
USB Parameter · 43, 44
  Delete · 44
USB Parameter Template · 42, 44, 45
  Add · 44
  Delete · 45
USB URB Data Source Dialog · 11
User Defined Stacks · 92
Using BPF · 277
Using Named Filters · 289
Utilization Table · 141

V

Values · 139
Viewing Data Events · 101

W

What To Do When The Correct Values Of Decoder
  Parameters Are Unknown · 80
Wi-Fi Timeline
  Channel Frequencies · 188
  Channel Frequencies - 5 GHz Channels · 189

Z

Zooming
  Zooming · 200